No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Richmond Division (The Hon. M. Hannah Lauck)

JOINT APPENDIX

VOLUME 1 of 11 (pages 1 - 176)

JESSICA D. ABER
United States Attorney

Kenneth R. Simon, Jr., Ass't U.S. Attorney
Peter S. Duffey, Ass't U.S. Attorney
Counsel for Appellee
919 East Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400

Nathan P. Judish, Senior Counsel
Computer Crime & Intel. Property Section
Criminal Division
U.S. Department of Justice

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
Counsel for Appellant
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800

Michael W. Price, Litigation Dir.
NACDL Fourth Amendment Ctr.
1660 L Street NW, 12th Floor
Washington, DC 20036

This page intentionally left blank for double-sided pagination and printing

TABLE OF CONTENTS

VOLUME 1 (pages 1 - 176)

District Court Docket Sheet (as of Jan. 17, 2023) 1

Indictment (Sept. 17, 2019, Doc. 1) 22

Defendant's Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Oct. 29, 2019, Doc. 29) 25

Government's Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (Nov. 19, 2019, Doc. 41) 51

Defendant's Reply to Government's Response [to] Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Dec. 9, 2019, Doc. 48) 76

Exh. A (First Step 2 Request to Google) (Doc. 48-1) 98
Exh. B (Second Step 2 Request to Google) (Doc. 48-2) 100
Exh. C (Third Step 2 Request to Google) (Doc. 48-3) 102
Exh. D (Transcript, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019)) (Doc. 48-4) ..... omitted from J.A.

Government's Notice Regarding Attachment of Google Geofence State Search Warrant to Response in Opposition to Motion to Suppress (Dec. 18, 2019, Doc. 54) 104

Affidavit for search warrant and warrant, with attachments (Doc. 54-1) 107

Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant (Dec. 20, 2019, Doc. 59-1) 118

United States' Response to Amicus Curiae Brief of Google LLC (Jan. 10, 2020, Doc. 71) 148

Defendant's Response to Google's Motion to File Amicus Curiae Brief in Support of Neither Party (Jan. 10, 2020, Doc. 72) 158

VOLUME 2 (pages 177 - 416)

Transcript, Discovery Motion Hearing (Jan. 21, 2020, Doc. 81; *see* Doc. 77 (court minutes))....177

Preliminary matters....179

Def't witness Spencer McInvaille — Direct examination....193; Cross examination....283; Redirect examination....306

Argument by the defense....318
Argument by the government....332
Rebuttal by the defense....350

Court's ruling....355

Defendant's Supplemental Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (May 22, 2020, Doc. 104)....363

United States' Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (June 12, 2020, Doc. 109)....393

VOLUME 3 (pages 417 - 694)

Transcript, Suppression Motion Hearing, Day 1 (evidence) (Mar. 4, 2021, Doc. 201; *see* Doc. 198 (court minutes))....417

Preliminary matters....420

Def't witness Spencer McInvaille — Direct examination....432; Cross examination....542; Redirect examination....586

Def't witness Marlo McGriff — Direct examination....606

VOLUME 4 (pages 695 - 1070)

Transcript, Suppression Motion Hearing, Day 2 (evidence) (Mar. 5, 2021, Doc. 202; *see* Doc. 199 (court minutes)) 695

Preliminary matters 698

Def't witness Marlo McGriff, cont'd — Direct examination ..... 699; Cross examination ..... 791; Redirect examination 841

Def't witness Sarah Rodriguez — Direct examination ..... 862; Cross examination ..... 902; Redirect examination 916

Gov't witness Jeremy D'Errico — Direct examination ..... 923; Cross examination ..... 967; Redirect examination 1010

Gov't witness Joshua Hylton — Direct examination ..... 1016; Cross examination ..... 1040; Redirect examination 1063

Concluding matters 1064

VOLUME 5 (pages 1071 - 1326)

Defendant's Post-Hearing Brief on "Geofence" General Warrant (May 3, 2021, Doc. 205) 1071

Government's Response in Opposition to Defendant's Motion for Suppression (May 21, 2020, Doc. 214; *see* Doc. 207-2) 1117

Defendant's Reply to Government's Response in Opposition to Motion for Suppression (June 4, 2020, Doc. 213) 1164

Transcript, Suppression Hearing (arguments) (June 24, 2021, Doc. 217; *see* Doc. 215 (court minutes)) 1185

Argument by the defense 1187
Argument by the government 1231
Rebuttal by the defense 1313

Concluding matters 1322

VOLUME 6 (pages 1327 - 1456)

Memorandum Opinion (denying suppression motion) (Mar. 3, 2022, Doc. 220) 1327

Order (denying suppression motion) (Mar. 3, 2022, Doc. 221) 1390

Criminal Information (May 6, 2022, Doc. 224) 1391

Transcript, Change of Plea Hearing (May 9, 2022, Doc. 247; *see* Doc. 226) 1394

Plea Agreement (May 9, 2022, Doc. 228) 1428

Statement of Facts (May 9, 2022, Doc. 229) 1444

Judgment in a Criminal Case (Aug. 19, 2022, Doc. 239) 1449

Notice of Appeal (Aug. 25, 2022, Doc. 241) 1456

VOLUME 7 (pages 1457 - 1810) – DOCUMENT EXHIBITS

Exhibits Admitted at Discovery Motion Hearing (Jan. 21, 2020)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) ..... *see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) ..... *see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) ..... *see* J.A. 2093
Def't Exh. 4: Activation Video ..... omitted from J.A., available on request
Def't Exh. 5: Three Paths Video (sealed) ..... *see* J.A. 2139
Def't Exh. 6: First Step 2 Request to Google 1457
Def't Exh. 7: Second Step 2 Request to Google 1459
Def't Exh. 8: Third Step 2 Request to Google 1461

Def't Exh. 9: Step 3 Request to Google 1463

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) .....*see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) .....*see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) .....*see* J.A. 2093
Def't Exh. 5: Three Paths Video (sealed) .....*see* J.A. 2139
Def't Exh. 6: Spencer McInvaille Report 1464
Def't Exh. 7: Spencer McInvaille Supplemental Report 1469
Def't Exh. 8: CSV Google Data File (.csv file) .....*see* J.A. 2139
Def't Exh. 9: Unique in Crowd Study 1475
Def't Exh. 11: September 2018 Oracle Submission 1480
Def't Exh. 18: Federal Search Warrant Application & Attachments 1502
Def't Exh. 19: State Search Warrants & Attachments 1534
Def't Exh. 21: McGriff Declaration 1 (Doc. 96-1) 1551
Def't Exh. 23: McGriff Declaration 3 (Doc. 147) 1562
Def't Exh. 24: Rodriguez Declaration (Doc. 96-2) 1579
Def't Exh. 27: Every Step You Take 1587
Def't Exh. 30: AZ Ex. 18 (admitted portions only) 1631
Def't Exh. 31: AZ Ex. 19 (admitted portions only) 1633
Def't Exh. 32: AZ Ex. 20 1639
Def't Exh. 33: AZ Ex. 24 1644
Def't Exh. 34: AZ Ex. 202 1667
Def't Exh. 36: AZ Ex. 209 1777
Def't Exh. 38: AZ Ex. 219 1781
Def't Exh. 40: AZ Ex. 236 1797
Def't Exh. 41: AZ Ex. 260 1804

VOLUME 8 (pages 1811 - 2090) – DOCUMENT EXHIBITS, CONT'D

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021), cont'd

Def't Exh. 43: May 2018 Privacy Policy – Redline 1811
Def't Exh. 43a: May 2018 Privacy Policy – Redline (with internet source information) 1840
Def't Exh. 44: Jan. 2019 Privacy Policy – Redline 1865
Def't Exh. 45: Oct. 2019 Privacy Policy – Redline 1895
Def't Exh. 46: McGriff Blog 1 1926

Def't Exh. 47: McGriff Blog 2 1929
Def't Exh. 48: 2018 Quartz Article 1934
Def't Exh. 49: 2018 AP Article 1 1941
Def't Exh. 51: 2019 NYT Article 1948
Def't Exh. 53: Blumenthal-Markey Letter to FTC 1957

Gov't Exh. 1: CAST PowerPoint Presentation 1981
Gov't Exh. 2: Geofence Warrant (Doc. 54-1) ..... *see* J.A. 107
Gov't Exh. 3: Declaration of Marlo McGriff (Mar. 11, 2020)
(same as Def't Exh. 21 (Doc. 96-1)) ..... *see* J.A. 1551
Gov't Exh. 3a: Declaration of Sarah Rodriguez (Mar. 11, 2020)
(same as Def't Exh. 24 (Doc. 96-2)) ..... *see* J.A. 1579
Gov't Exh. 3b: Supplemental Declaration of McGriff (June 17, 2020)
(Doc. 110-1) 2032
Gov't Exh. 3c: Third Declaration of Marlo McGriff (Aug. 7, 2020)
(same as Def't Exh. 23 (Doc. 147)) ..... *see* J.A. 1562
Gov't Exh. 4: Joshua Hylton emails with Google 2034
Gov't Exh. 5: Google Privacy Policy 2048
Gov't Exh. 5a: Google Terms of Service 2081
Gov't Exh. 6: Special Agent D'Errico's C.V. 2088
Gov't Exh. 12: "Got to Be Mobile" Video ..... *see* J.A. 2091

VOLUME 9 (pages 2091 - 2092) – DIGITAL MEDIA EXHIBIT

Gov't Exh. 12: "Got to Be Mobile" Video (admitted only at suppression motion hearing) ..... (.mp4 file)

VOLUME 10 (pages 2093 - 2138) – SEALED DOCUMENT EXHIBIT

Def't Exh. 3: PDF of Raw Data (*see* Doc. 69 (sealing order)) (admitted at both discovery motion hearing and suppression motion hearing) 2093

VOLUME 11 (pages 2139 - end) – SEALED DIGITAL MEDIA EXHIBITS

Def't Exh. 5: Three Paths Video (admitted at both discovery motion hearing and suppression motion hearing) ..... (.mp4 file)
Def't Exh. 8: CSV Google Data File (admitted only at suppression motion hearing) ..... (.csv file, viewable in Excel)

APPEAL,CLOSED

U.S. District Court
Eastern District of Virginia − (Richmond)
CRIMINAL DOCKET FOR CASE #: 3:19−cr−00130−MHL−1

Case title: USA v. Chatrie

Date Filed: 09/17/2019
Date Terminated: 08/19/2022

Assigned to: District Judge M. Hannah Lauck

Appeals court case number: 22−4489

Defendant (1)

Okello T. Chatrie
TERMINATED: 08/19/2022

represented by **Laura Jill Koenig**
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
(804) 343−0800
Email: laura_koenig@fd.org
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Public Defender

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
NA
(202) 465−7615
Fax: (202) 872−8690
Email: mprice@nacdl.org
PRO HAC VICE
ATTORNEY TO BE NOTICED
Designation: Public Defender

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
804−343−0800
Email: Paul_Gill@fd.org
ATTORNEY TO BE NOTICED

Pending Counts	**Disposition**
18;2113(a), 2113(d) and 2113(e); In accordance with 18;924(d) and 981(a)(1)(C) as incorporated by 28;2461(c) − FORCED ACCOMPANIMENT DURING AN ARMED CREDIT UNION ROBBERY; FORFEITURE ALLEGATION (1)	DISMISSED ON MOTION OF GOVT.

18 U.S.C. §§ 2113(a) and 2113(d); ARMED CREDIT UNION ROBBERY; FORFEITURE ALLEGATION (1s)	57 MONTHS IMPRISONMENT, 3 YEARS SUPERVISED RELEASE, $100 S/A, $196,932.01 RESTITUTION
18;924(c)(1)(A)(i) and (ii); In accordance with 18;924(d) and 981(c)(1)(C) as incorporated by 28;2461(c) − USE, CARRY AND BRANDISH A FIREARM DURING AND IN RELATION TO A CRIME OF VIOLENCE; FORFEITURE ALLEGATION (2)	DISMISSED ON MOTION OF GOVT.
18 U.S.C. § 924(c)(1)(A)(i) and (ii); USE, CARRY, AND BRANDISH A FIREARM DURING AND IN RELATION TO A CRIME OF VIOLENCE; FORFEITURE ALLEGATION (2s)	84 MONTHS IMPRISONMENT TO BE SERVED CONSECUTIVE TO CT. 1, 3 YEARS SUPERVISED RELEASE TO BE SERVED CONCURRENT TO CT. 1, $100 S/A

Highest Offense Level (Opening)

Felony

Terminated Counts	**Disposition**
None	

Highest Offense Level (Terminated)

None

Complaints	**Disposition**
None	

Movant

Google, LLC
TERMINATED: 08/19/2022

represented by **Brittany Blueitt Amadi**
Wilmer Cutler Pickering Hale & Dorr LLP (DC)
1875 Pennsylvania Ave NW
Washington, DC 20006
202−663−6022
Fax: 202−663−6363
Email: brittany.amadi@wilmerhale.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Retained

Alex Campbell Hemmer
Wilmer Cutler Pickering Hale & Dorr LLP (DC−NA)
1875 Pennsylvania Ave NW
Washington, DC 20006
NA
(202) 663−6387
Fax: (202) 663−6363
Email: alex.hemmer@wilmerhale.com

TERMINATED: 01/19/2021
PRO HAC VICE
Designation: Retained

Catherine Mary Agnes Carroll
Wilmer Cutler Pickering Hale & Dorr, LLP (DC)
1875 Pennsylvania Avenue NW
Washington, DC 20006
202−663−6000
Fax: 202−663−6363
Email: Catherine.Carroll@wilmerhale.com
ATTORNEY TO BE NOTICED
Designation: Retained

Movant

Magistrate Judge David M. Bishop
TERMINATED: 08/19/2022

represented by **Rachel Lynsie Yates**
Office of the Attorney General
202 North 9th Street
Richmond, VA 23219
804−692−0552
Email: ryates@oag.state.va.us
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Retained

Donald Eldridge Jeffrey , III
Office of the Attorney General
202 North 9th Street
Richmond, VA 23219
(804) 786−2071
Email: djeffrey@oag.state.va.us
ATTORNEY TO BE NOTICED

Plaintiff

USA

represented by **Kenneth R. Simon , Jr.**
United States Attorney's Office (Richmond)
SunTrust Building
919 East Main Street
Suite 1900
Richmond, VA 23219
(804) 819−5400
Email: Kenneth.Simon2@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: US Attorney

Nathan Paul Judish
United States Department of Justice Computer Crime and Intellectual Property Section
950 Pennsylvania Ave NW
Washington, DC 20530
NA
(202) 616−7203
Fax: (202) 514−6113
Email: nathan.judish@usdoj.gov
PRO HAC VICE
ATTORNEY TO BE NOTICED
Designation: US Attorney

Peter S. Duffey
United States Attorney's Office
(Richmond)
SunTrust Building
919 East Main Street
Suite 1900
Richmond, VA 23219
(804) 819−5400
Email: peter.duffey@usdoj.gov
ATTORNEY TO BE NOTICED
Designation: US Attorney

Date Filed	#	Docket Text
09/17/2019	1	INDICTMENT as to Okello T. Chatrie (1) counts 1, 2. (smej,) (Entered: 09/18/2019)
09/17/2019	3	Minute Entry as to Okello T. Chatrie: Before Magistrate Judge David J. Novak. Appearances: Stephen Miller, AUSA and Sheldon Poe, GJR. Indictment, a true bill, returned before a Magistrate Judge at Richmond. Government's motion for the issuance of an arrest warrant heard and so−ordered. (smej,) (Entered: 09/18/2019)
09/18/2019	4	Arrest Warrant Issued (as detainer) in case as to Okello T. Chatrie. Clerk placed in USM box for service. (smej,) (Entered: 09/18/2019)
09/20/2019	5	Petition and Order for Writ of Habeas Corpus ad Prosequendum as to Okello T. Chatrie for September 26, 2019 at 2:05 P.M.. Signed by Magistrate Judge David J. Novak on 09/20/2019. (smej,) (Entered: 09/20/2019)
09/20/2019	6	Writ of Habeas Corpus ad Prosequendum Issued as to Okello T. Chatrie for 09/26/2019 at 2:05 P.M.. Clerk placed in USM box for service. (smej,) (Entered: 09/20/2019)
09/26/2019		Oral ORDER APPOINTING FEDERAL PUBLIC DEFENDER as to Okello T. Chatrie. Laura Jill Koenig for Okello T. Chatrie appointed by Magistrate Judge David J. Novak on 9/26/2019. (cgar) (Entered: 09/26/2019)
09/26/2019	8	Minute Entry for proceedings held before Magistrate Judge David J. Novak:Initial Appearance as to Okello T. Chatrie held on 9/26/2019. Matter came on for initial appearance on Indictment. Deft advised of charges/penalties and rights. Deft requested c/a counsel. Financial affidavit executed. Carolyn V. Grady, AFPD present. FPD appointed. Govt's motion to detain deft GRANTED. Detention hearing set for 10/1/2019 at 2:05. Arraignment set for 10/1/2019 at 2:30 p.m. Deft remanded to custody. (Tape #FTR.)(cgar) (Entered: 09/26/2019)
09/26/2019		Set Hearings as to Okello T. Chatrie: Arraignment set for 10/1/2019 at 02:30 PM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. Detention Hearing set for 10/1/2019 at 02:05 PM in Richmond Courtroom 5400 before Magistrate Judge David J. Novak. (cgar) (Entered: 09/26/2019)
09/26/2019	9	CJA 23 Financial Affidavit by Okello T. Chatrie. (cgar) (Entered: 09/26/2019)
09/26/2019	10	ARREST Warrant Returned Executed on 9/26/2019 as to Okello T. Chatrie. (cgar) (Entered: 09/26/2019)
09/26/2019	11	Temporary Detention Order as to Okello T. Chatrie. Signed by Magistrate Judge David J. Novak on 9/26/2019. (cgar) (Entered: 09/27/2019)
10/01/2019	12	Minute Entry for proceedings held before Magistrate Judge David J. Novak:Detention Hearing as to Okello T. Chatrie held on 10/1/2019. Matter came on for detention hearing. Deft waived detention hearing. Waiver executed. Arraignment set for today at 2:30 p.m. Deft ordered held pending trial. (Tape #FTR.)(cgar) (Entered: 10/01/2019)
10/01/2019	13	WAIVER of Detention Hearing by Okello T. Chatrie. (cgar) (Entered: 10/01/2019)
10/01/2019	14	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Arraignment as to Okello T. Chatrie (1) Count 1,2 held on 10/1/2019. Dft waived formal reading of the Indictment, entered a plea of not guilty and requested a

		trial by jury. Agreed Discovery Order entered. Jury Trial scheduled for December 3−5, 2019 at 9:00 a.m. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 10/02/2019)
10/01/2019	15	Agreed Discovery Order as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 10/1/19. (khan,) (Entered: 10/02/2019)
10/01/2019	16	Detention Order Pending Trial as to Okello T. Chatrie. Signed by Magistrate Judge David J. Novak on 10/1/2019. (cgar) (Entered: 10/02/2019)
10/02/2019		Set/Reset Hearings as to Okello T. Chatrie: Jury Trial set for 12/3/2019 at 09:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 10/02/2019)
10/22/2019	17	MOTION in Limine *of Irrelevant and Unduly Prejudicial Character Evidence* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	18	MOTION to Suppress *Evidence Obtained from Willis Street Search* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	19	MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	20	MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	21	MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	22	MOTION to Suppress *Evidence Obtained from Cell Site Simulator* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	23	MOTION for Discovery *Regarding Government's Use of Cell Site Simulator* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	24	Consent MOTION for Extension *of Motions Deadline on One Issue that Will Result in Two Additional Motions* by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 10/22/2019)
10/23/2019	25	ORDER − It is hereby ORDERED that the Defendant's Motion to Extend Motions Deadline on One Issue Which Will Result in Two Additional Motions in this case is GRANTED. The defense shall file the two additional motions relating to the state search warrant using "geofencing" and Google's "sensorvault" data by October 29, 2019. The government's response deadline and the defense's reply deadline are adjusted accordingly. Signed by District Judge M. Hannah Lauck on 10/23/2019. (smej,) (Entered: 10/23/2019)
10/29/2019	26	Motion to appear Pro Hac Vice by Michael William Price and Certification of Local Counsel Laura Jill Koenig by Okello T. Chatrie. (Attachments: # 1 Proposed Order Pro Hac Vice Application)(Koenig, Laura) (Entered: 10/29/2019)
10/29/2019		Notice of Correction re 26 Motion to appear Pro Hac Vice by Michael William Price and Certification of Local Counsel Laura Jill Koenig: Clerk has notified filing attorney of proper filing procedures for pro hac vice motions. No further action is required. (smej,) (Entered: 10/29/2019)
10/29/2019	27	ORDER granting 26 Motion for Michael William Price to appear as Pro hac vice for Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 10/29/2019. (smej,) (Entered: 10/29/2019)
10/29/2019	28	MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/29/2019)
10/29/2019	29	MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/29/2019)
10/31/2019	30	Consent MOTION for Extension of Time to File Response/Reply as to 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data*, 17 MOTION in Limine *of Irrelevant and Unduly Prejudicial Character Evidence*, 18

		MOTION to Suppress *Evidence Obtained from Willis Street Search*, 20 MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search*, 19 MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search*, 21 MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search*, 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*, 23 MOTION for Discovery *Regarding Government's Use of Cell Site Simulator*, 22 MOTION to Suppress *Evidence Obtained from Cell Site Simulator* by USA as to Okello T. Chatrie. (Attachments: # 1 Proposed Order Proposed Order)(Simon, Kenneth) (Entered: 10/31/2019)
11/01/2019	31	ORDER as to Okello T. Chatrie that the Court GRANTS the United States' 30 motion for extension of time. Accordingly, the United States must respond to the defendant's motions on or before November 19, 2019. See Order for details. Signed by District Judge M. Hannah Lauck on 11/1/2019. (jsmi,) (Entered: 11/01/2019)
11/07/2019	32	ORDER − This matter comes before the Court on the Parties' joint request for a status hearing. At **11:00 a.m. on November 12, 2019**, the Parties SHALL appear in Courtroom 6100 of the Spottswood W. Robinson III and Robert R. Merhige, Jr. United States Courthouse for an in−person status conference to discuss the trial date in this matter. Signed by District Judge M. Hannah Lauck on 11/07/2019. (smej,) (Entered: 11/07/2019)
11/07/2019		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 11/12/2019 at 11:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 11/07/2019)
11/12/2019	33	NOTICE OF ATTORNEY APPEARANCE: Paul Geoffrey Gill appearing for Okello T. Chatrie (Gill, Paul) (Entered: 11/12/2019)
11/12/2019	34	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 11/12/2019. Oral Motion to Delay Reply until 12/9/19 − GRANTED. Dft's Motion for Continuance of Trial Beyond the Speedy Trial Act Cut−Off Date − GRANTED. Status Conference set 12/12/19 at 2:00 p.m. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 11/12/2019)
11/12/2019		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 12/12/2019 at 02:00 PM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 11/12/2019)
11/12/2019	35	MOTION for Continuance of Trial Beyond the Speedy Trial Act Cut−Off Date by Okello T. Chatrie. (khan,) (Entered: 11/18/2019)
11/12/2019		ORAL ORDER as to Okello T. Chatrie granting 35 MOTION for Continuance of Trial Beyond the Speedy Trial Act Cut−Off Date filed by Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 11/12/19. (khan,) (Entered: 11/18/2019)
11/19/2019	36	MOTION for Leave to File Excess Pages by USA as to Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	37	RESPONSE in Opposition by USA as to Okello T. Chatrie re 18 MOTION to Suppress *Evidence Obtained from Willis Street Search*, 19 MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search* (Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	38	RESPONSE in Opposition by USA as to Okello T. Chatrie re 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* (Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	39	RESPONSE to Motion by USA as to Okello T. Chatrie re 17 MOTION in Limine *of Irrelevant and Unduly Prejudicial Character Evidence* (Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	40	RESPONSE to Motion by USA as to Okello T. Chatrie re 23 MOTION for Discovery *Regarding Government's Use of Cell Site Simulator*, 22 MOTION to Suppress *Evidence Obtained from Cell Site Simulator* (Simon, Kenneth) (Entered: 11/19/2019)

11/19/2019	41	RESPONSE in Opposition by USA as to Okello T. Chatrie re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* (Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	42	RESPONSE in Opposition by USA as to Okello T. Chatrie re 20 MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search* (Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	43	RESPONSE in Opposition by USA as to Okello T. Chatrie re 21 MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search* (Simon, Kenneth) (Entered: 11/19/2019)
11/20/2019	44	ORDER − For good cause shown, the Court GRANTS the United States' 36 Motion for Leave to File Excess Pages. Accordingly, the United States may file its omnibus responsive brief that is in excess of thirty pages. Signed by District Judge M. Hannah Lauck on 11/20/2019. (smej,) (Entered: 11/20/2019)
11/25/2019	45	REPLY TO RESPONSE to by Okello T. Chatrie re 18 MOTION to Suppress *Evidence Obtained from Willis Street Search*, 19 MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search*, 37 Response in Opposition (Koenig, Laura) (Entered: 11/25/2019)
11/25/2019	46	REPLY TO RESPONSE to by Okello T. Chatrie re 20 MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search*, 42 Response in Opposition (Koenig, Laura) (Entered: 11/25/2019)
11/25/2019	47	REPLY TO RESPONSE to by Okello T. Chatrie re 43 Response in Opposition, 21 MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search* (Koenig, Laura) (Entered: 11/25/2019)
11/26/2019		Jury Trial continued as to Okello T. Chatrie: (khan,) (Entered: 11/26/2019)
12/09/2019	48	REPLY TO RESPONSE to by Okello T. Chatrie re 41 Response in Opposition (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D)(Koenig, Laura) (Entered: 12/09/2019)
12/09/2019	49	REPLY TO RESPONSE to by Okello T. Chatrie re 38 Response in Opposition (Koenig, Laura) (Entered: 12/09/2019)
12/11/2019	50	NOTICE *Regarding Initiation of Forensic Examination* by Okello T. Chatrie (Simon, Kenneth) (Entered: 12/11/2019)
12/12/2019	52	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 12/12/2019. Goggle Amicus brief due 12/20/19; parties response 1/3/20. Discovery motion scheduled 1/21/20 at 11:00 a.m.; Motion to Suppress scheduled 2/21 & 21/20 at 10:00 a.m. ECF 17, 22, 23 DENIED AS MOOT WITHOUT PREJUDICE. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 12/13/2019)
12/13/2019	51	ORDER − The Court DENIES AS MOOT and WITHOUT PREJUDICE Defendant Okello T. Chatrie's Motion in Limine 17 , Motion to Suppress 22 , and Motion for Discovery 23 ; SCHEDULES this matter for a hearing on **January 21, 2020, at 11:00 a.m.** regarding Chatrie's Motion for Discovery Regarding Government's Use of Google's Sensorvault Data 28 ; SCHEDULES this matter for a hearing, beginning at **10:00 a.m. on February 20, 2020, and continuing through February 21, 2020** regarding Chatrie's remaining pending motions, (ECF Nos. 18 , 19 , 20 , 21 , 29). SEE ORDER FOR DETAILS AND DEADLINES. Signed by District Judge M. Hannah Lauck on 12/13/2019. (smej,) (Entered: 12/13/2019)
12/13/2019		Set/Reset Hearings as to Okello T. Chatrie: Discovery Hearing set for 1/21/2020 at 11:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 12/13/2019)
12/13/2019		Set/Reset Deadlines re Motion or Report and Recommendation in case as to Okello T. Chatrie 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*, 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data*, 21 MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search*, 18 MOTION to Suppress *Evidence Obtained from Willis Street Search*, 19 MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search*. Motion

		Hearing set for 2/20/2020 at 10:00 AM before District Judge M. Hannah Lauck. (khan,) (Entered: 12/13/2019)
12/16/2019	53	ORDER − This matter comes before the Court on Defendant Okello T. Chatrie's Motion for Discovery Regarding Government's Use of Google's Sensorvault Data 28 . In Chatrie's reply to the United States' response to this motion, 49 , Chatrie raises several new arguments. Because a response to these new arguments from the United States would assist the Court, the United States SHALL file a sur−reply−no longer than 10 pages−no later than December 30, 2019. Signed by District Judge M. Hannah Lauck on 12/16/2019. (smej,) (Entered: 12/16/2019)
12/18/2019	54	NOTICE *of Attachment to Response in Opposition to Motion to Suppress − Google Geofence State Search Warrant* by USA as to Okello T. Chatrie re 48 Reply to Response, 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*, 41 Response in Opposition (Attachments: # 1 Exhibit)(Simon, Kenneth) (Entered: 12/18/2019)
12/19/2019	55	STATUS REPORT *regarding Filing of Search Warrants at Issue in this Matter* by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 12/19/2019)
12/19/2019		Minute Entry for proceedings held before District Judge M. Hannah Lauck:Telephone Conference as to Okello T. Chatrie held on 12/19/2019 (Court Reporter Gil Halasz, OCR.)(khan,) (Entered: 12/19/2019)
12/19/2019	56	RESPONSE by Okello T. Chatrie re 55 Status Report (Koenig, Laura) (Entered: 12/19/2019)
12/20/2019	57	Motion to appear Pro Hac Vice by Catherine Carroll and Certification of Local Counsel Brittany Amadi (Filing fee $ 75 receipt number 0422−6996925.) by Google, LLC as to Okello T. Chatrie. (Amadi, Brittany) (Entered: 12/20/2019)
12/20/2019	58	Motion to appear Pro Hac Vice by Alex Hemmer and Certification of Local Counsel Brittany Amadi (Filing fee $ 75 receipt number 0422−6996939.) by Google, LLC as to Okello T. Chatrie. (Amadi, Brittany) (Entered: 12/20/2019)
12/20/2019	59	MOTION to File Amicus Brief *In Support Of Neither Party* by Brittany Amadi. by Google, LLC as to Okello T. Chatrie. (Attachments: # 1 Amicus Brief, # 2 Proposed Order)(Amadi, Brittany) (Entered: 12/20/2019)
12/23/2019	60	ORDER Granting Motion for Leave to File Brief of Amicus Curiae Google LLC in Support of Neither Party. Having considered the motion of proposed amicus curiae Google LLC for leave to file an arnicus brief, and good cause appearing, it is hereby ORDERED that the motion is GRANTED. The Clerk is directed to accept the proposed arnicus brief for filing. SO ORDERED. Signed by District Judge M. Hannah Lauck on 12/23/2019. (sbea,) (Entered: 12/23/2019)
12/23/2019	61	REPLY TO RESPONSE to USA as to Okello T. Chatrie re 56 Response *to Status Report regarding Filing Search Warrants at Issue* (Simon, Kenneth) (Entered: 12/23/2019)
12/23/2019	73	Amicus Brief by Google, LLC as to Okello T. Chatrie. Filed per Order entered 12/23/2019. (smej,) Modified on 1/13/2020 (smej,). (Entered: 01/13/2020)
12/30/2019	62	ORDER granting 57 Motion for Catherine Mary Agnes Carroll to appear as Pro hac vice for Google, LLC as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 12/27/2019. (smej,) (Entered: 12/30/2019)
12/30/2019	63	ORDER granting 58 Motion for Alex Campbell Hemmer to appear as Pro hac vice for Google, LLC as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 12/27/2019. (smej,) (Entered: 12/30/2019)
12/30/2019	64	Supplemental Memorandum by USA as to Okello T. Chatrie re 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* (Simon, Kenneth) (Entered: 12/30/2019)
12/30/2019	65	ORDER that this matter comes before the Court on the United States of America's Status Report Regarding Filing Search Warrants at Issue in this Matter 55 . Given the disagreement expressed in the parties' filings, Counsel for both parties, along with their supervisors, SHALL appear for an in−person status conference on January 8, 2020 at

		2:30 p.m.as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 12/30/19. (jtho,) (Entered: 12/30/2019)
12/30/2019		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 1/8/2020 at 02:30 PM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 12/30/2019)
12/31/2019	66	Consent MOTION for Extension of Time to File Response/Reply as to 51 Order on Motion in Limine,,, Order on Motion to Suppress,,, Order on Motion for Discovery,, 59 MOTION to File Amicus Brief *In Support Of Neither Party* by Brittany Amadi. by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 12/31/2019)
12/31/2019	67	ORDER − Upon motion of defense counsel, with good cause having been shown and noting no objection by the Government it is hereby ORDERED that the Defendant's Motion to Extend Deadline to Respond to Google's Amicus Brief in this case is GRANTED. The parties must file any response to Google's Brief of Amicus Curiae by January 10, 2020. Signed by District Judge M. Hannah Lauck on 12/31/2019. (smej,) (Entered: 12/31/2019)
01/03/2020	68	MOTION to Seal *Raw Data Returns Provided by Google* by Okello T. Chatrie. (Koenig, Laura) (Entered: 01/03/2020)
01/07/2020	69	ORDER − The Court GRANTS the Motion to Seal 68 . The Court DIRECTS the Clerk to file Exhibit A to the Motion to Seal, the raw returns, under seal. The Court CANCELS the January 8, 2020 Status Conference. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 1/7/2020. (smej,) (Entered: 01/07/2020)
01/07/2020		Status hearing as to Okello T. Chatrie on 1/8/20 CANCELLED. (khan,) (Entered: 01/07/2020)
01/10/2020	71	RESPONSE by USA as to Okello T. Chatrie re 73 Amicus Brief. (Simon, Kenneth) Modified on 1/13/2020 (smej,). Modified on 1/13/2020 (smej,). (Entered: 01/10/2020)
01/10/2020	72	RESPONSE in Opposition to Motion by Okello T. Chatrie re 59 MOTION to File Amicus Brief *In Support Of Neither Party*. (Koenig, Laura) Modified to correct docket text on 1/13/2020 (smej,). (Entered: 01/10/2020)
01/13/2020		Notice of Correction re 73 Amicus Brief: Amicus Brief filed by the Clerk as of the date the Order 60 was entered on 12/23/2019. Relationship between docket entry 73 and 71 has been corrected. (smej,) (Entered: 01/13/2020)
01/21/2020	76	*Defendant's Proposed* EXHIBIT LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 01/21/2020)
01/21/2020	77	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Motion Hearing as to Okello T. Chatrie held on 1/21/2020 re 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* filed by Okello T. Chatrie. Motion to SEAL − GRANTED. Dft adduced evidence, RESTED. Govt. RESTED. Arguments heard. Court findings −− additional briefing due 1/24/20. Cross motions due 2/18/20 − cross responses due 2/25. Hearing to be scheduled once the Court has all of the information. Motion to Suppress scheduled 2/20 & 21/20 is continued. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 01/22/2020)
01/22/2020	78	ORDER − The Court: ORDERS the Parties to file, no later than January 24, 2020, a statement regarding the Chesterfield County magistrate who signed the June 14, 2019 Geofence Warrant; ORDERS Chatrie to provide, no later than February 10, 2020, expert disclosures of any proposed experts Chatrie intends to call at the hearing on the Motions to Suppress; CANCELS the February 20−21, 2020 Hearing on the Motions to Suppress. To the extent this this Order conflicts with the Court's December 13, 2019 Order, 51 , this Order SHALL supersede the December 13, 2019 Order. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 1/22/2020. (smej,) (Entered: 01/22/2020)

01/22/2020		Discovery Motion held as to Okello T. Chatrie: (khan,) (Entered: 01/22/2020)
01/24/2020	79	STIPULATION by Okello T. Chatrie *(Joint Stipulation with the Government)* (Koenig, Laura) (Entered: 01/24/2020)
01/30/2020	81	TRANSCRIPT of Proceedings held on January 21, 2020, before Judge M. Hannah Lauck. Court reporter Diane Daffron, Telephone number 804−916−2893. **NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 3/2/2020. Redacted Transcript Deadline set for 3/31/2020. Release of Transcript Restriction set for 4/29/2020.(daffron, diane) (Entered: 01/30/2020)**
02/04/2020	82	MOTION for Issuance of Subpoenas *Duces Tecum* and Memorandum in Support by Okello T. Chatrie. (Attachments: # 1 Proposed Order) (Koenig, Laura) Modified docket text on 2/5/2020 (smej,). (Entered: 02/04/2020)
02/07/2020	83	ORDER − Although the United States has until February 18, 2020, to file its response pursuant to Local Rule 7(F) for the United States District Court for the Eastern District of Virginia, in the interests of justice and because the United States has previously suggested that Chatrie pursue a Rule 17 subpoena, the United States SHALL file a response to the Motion for Subpoena no later than February 11, 2020. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 2/7/2020. (smej,) (Entered: 02/07/2020)
02/07/2020	84	RESPONSE to Motion by USA as to Okello T. Chatrie re 82 MOTION for Issuance of Subpoenas *Duces Tecum* (Simon, Kenneth) (Entered: 02/07/2020)
02/07/2020	85	ORDER (Granting Defendant's Motion for Issuance of Subpoena Duces Tecum) − Defendant's Motion for Issuance of Subpoena Duces Tecum 82 , pursuant to Fed. R. Crim. P. 17(c), requiring production of the states document(s), is GRANTED. SEE ORDER FOR DETIALS. Signed by District Judge M. Hannah Lauck on 2/7/2020. (smej,) (Entered: 02/07/2020)
02/07/2020	86	Subpoena Duces Tecum Issued as to Google, LLC 82 . Clerk placed in USM box for service. (smej,) (Entered: 02/07/2020)
02/18/2020	87	Supplemental Memorandum by Okello T. Chatrie re 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* (Attachments: # 1 Exhibit A (CellHawk template), # 2 Exhibit B)(Koenig, Laura) (Entered: 02/18/2020)
02/18/2020	88	Supplemental Memorandum by USA as to Okello T. Chatrie re 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* (Simon, Kenneth) (Entered: 02/18/2020)
02/20/2020	89	MOTION to Defer Google's Subpoena Compliance Deadline to Close of Business on Friday, March 6, 2020 re 85 Order on Motion for Issuance of Subpoenas, 86 Subpoena(s) Issued by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 02/20/2020)
02/21/2020	90	ORDER − Upon motion of defense counsel, with good cause having been shown, it is hereby ORDERED that the Defendant's Motion to Defer Google's Subpoena Compliance Deadline to Close of Business on Friday, March 6, 2020, in this case is GRANTED. The time in which Google must comply with the February 7, 2020, subpoena duces tecum in ECF No. 86 is deferred to Friday, March 6, 2020, by the close of business Eastern Standard Time. Signed by District Judge M. Hannah Lauck on 2/21/2020. (smej,) (Entered: 02/21/2020)
02/24/2020	91	Subpoena Returned on 2/12/2020 re 86 Subpoena Duces Tecum Issued. (smej,) Modified to correct docket text on 2/25/2020. Incorrect docket event selected (smej,). (Entered: 02/25/2020)

02/25/2020	92	RESPONSE by Okello T. Chatrie re 88 Supplemental Memorandum (Koenig, Laura) (Entered: 02/25/2020)
02/25/2020	93	RESPONSE by USA as to Okello T. Chatrie re 87 Supplemental Memorandum (Simon, Kenneth) (Entered: 02/25/2020)
03/06/2020	94	Second MOTION re 85 Order on Motion for Issuance of Subpoenas, 90 Order on Motion for Miscellaneous Relief,, by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 03/06/2020)
03/06/2020	95	ORDER granting 94 Motion as to Okello T. Chatrie (1): Upon motion of defense counsel, with good cause having been shown, it is hereby ORDERED that the Defendant's Second Motion to Defer Google's Subpoena Compliance Deadline to Close of Business on Wednesday, March 11, 2020, in this case is GRANTED; thetime in which Google must comply with the February 7,2020, subpoena duces tecum in EOF No. 86 is deferred to Wednesday, March 11, 2020, by the close of business Eastern Standard Time (signed by District Judge M. Hannah Lauck on 3/6/2020) (rpiz) (Entered: 03/06/2020)
03/11/2020	96	RESPONSE by Google, LLC as to Okello T. Chatrie re 95 Order on Motion for Miscellaneous Relief,, (Attachments: # 1 Attachment A, # 2 Attachment B)(Amadi, Brittany) (Entered: 03/11/2020)
03/12/2020	97	NOTICE *of Satisfaction with Google Response to Subpoena Duces Tecum* by Okello T. Chatrie re 96 Response, 86 Subpoena(s) Issued (Koenig, Laura) (Entered: 03/12/2020)
03/25/2020	98	ORDER − Chatrie SHALL file a statement regarding the effect of Google's response to the subpoena on the pending Motion for Discovery. Chatrie's statement SHALL identify which discovery requests (by number or subpart, when applicable) have been fulfilled and which remain unsatisfied. Because Chatrie has received responsive information from Google, he SHALL also identify whether he continues to argue that Google is a member of the prosecution team under either Rule 16 of the Federal Rules of Criminal Procedure or the Supreme Court of the United States' decision in Brady v. Maryland, 373 U.S. 83 (1963). Chatrie SHALL file this statement no later than April 10, 2020, and SHALL limit his response to no more than three (3) pages. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 3/25/2020. (smej,) (Entered: 03/25/2020)
04/10/2020	99	NOTICE *of Satisfaction of Requests in Geofence Discovery Motion* by Okello T. Chatrie re 98 Order,,, (Koenig, Laura) (Entered: 04/10/2020)
04/13/2020	100	RESPONSE by USA as to Okello T. Chatrie re 99 Notice (Other) (Simon, Kenneth) (Entered: 04/13/2020)
04/13/2020	101	ORDER that the Court DENIES as MOOT the Motion for Discovery (ECF No. 28) and SCHEDULES an in person hearing on Geofence Motion to Suppress (ECF No. 29) on July 2, 2020 at 9:30 a.m. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 4/13/20. (khan,) (Entered: 04/13/2020)
04/13/2020		Set/Reset Deadlines re Motion or Report and Recommendation in case as to Okello T. Chatrie 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*. Motion Hearing set for 7/2/2020 at 09:30 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 04/13/2020)
05/12/2020	102	Consent MOTION for Extension *of Supplemental Briefing Deadlines* by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 05/12/2020)
05/13/2020	103	ORDER − It is hereby ORDERED that the Defendants Motion to Extend Supplemental Briefing on Geofence Motion to Suppress By One Week, in this case is GRANTED. Mr. Chatrie must file his supplement to his Geofence Motion to Suppress by May 22, 2020. The governments supplemental response deadline is extended to June 5, 2020. Signed by District Judge M. Hannah Lauck on 5/13/2020. (smej,) (Entered: 05/13/2020)
05/22/2020	104	Supplemental Memorandum by Okello T. Chatrie re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* (Koenig, Laura) (Entered: 05/22/2020)

05/26/2020	105	Motion to appear Pro Hac Vice by Nathan Judish and Certification of Local Counsel Kenneth Simon, Jr. by USA as to Okello T. Chatrie. (Simon, Kenneth) (Entered: 05/26/2020)
05/28/2020	106	Consent MOTION for Extension of Time to File Response/Reply as to 104 Supplemental Memorandum by USA as to Okello T. Chatrie. (Attachments: # 1 Proposed Order Proposed Order)(Simon, Kenneth) (Entered: 05/28/2020)
05/28/2020	107	ORDER granting 105 Motion for Nathan Paul Judish to appear as Pro hac vice for USA. Signed by District Judge M. Hannah Lauck on 5/28/2020. (smej,) (Entered: 05/28/2020)
05/28/2020	108	ORDER − Upon Motion of the United States of America, by and through attorneys. G. Zachary Terwilliger. United States Attorney for the Eastern District of Virginia, Kenneth R. Simon, Jr. and Peter S. Duffey. Assistant United States Attorneys, for an extension of time to file a response to the defendant's supplemental memorandum in support of his motion to suppress 104 from June 5, 2020 to June 12, 2020, and the defendant having no objection and for good cause shown, the Court GRANTS the United States' motion. Accordingly, the United States must respond to the defendant's motions on or before June 12, 2020. Signed by District Judge M. Hannah Lauck on 5/28/2020. (smej,) (Entered: 05/28/2020)
06/12/2020	109	RESPONSE by USA as to Okello T. Chatrie re 104 Supplemental Memorandum (Simon, Kenneth) (Entered: 06/12/2020)
06/17/2020	110	MOTION for Leave to File *Supplemental Declaration of Marlo McGriff* by Google, LLC as to Okello T. Chatrie. (Attachments: # 1 Supplemental Declaration of Marlo McGriff, # 2 Proposed Order)(Amadi, Brittany) (Entered: 06/17/2020)
06/22/2020	111	Objection by Okello T. Chatrie re 110 MOTION for Leave to File *Supplemental Declaration of Marlo McGriff and Motion to Strike Such Declaration* (Koenig, Laura) (Entered: 06/22/2020)
06/24/2020	115	MEMORANDUM ORDER − This matter comes before the Court on Google LLC's ("Google ") Motion for Leave to File Supplemental Declaration of Marlo McGriff (the "Motion ") 110 . The Court GRANTS the Motion, 110 ; CONTINUES GENERALLY the July 2, 2020 Hearing on Chatrie's Geofence Motion to Suppress. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 6/24/2020. (smej,) (Entered: 06/24/2020)
06/24/2020	116	ORDER − The Parties SHALL file no later than July 8, 2020, a statement, not to exceed ten (10) pages, on these effects, if any. If they so choose, the Parties SHALL file no later than July 15, 2020, a response, not to exceed ten (10) pages, to the other party's statement. The Parties SHALL address any additional information they have gained about Mr. Bishop in their initial position statements. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 6/24/2020. (smej,) (Entered: 06/24/2020)
06/26/2020	117	*Motion to Suppress GeoFence Search Warrant* WITNESS LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 06/26/2020)
06/26/2020	118	*Motion to Suppress GeoFence Search Warrant* EXHIBIT LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 06/26/2020)
06/26/2020	119	*Preliminary* EXHIBIT LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 06/26/2020)
06/26/2020	120	*Preliminary* WITNESS LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 06/26/2020)
07/02/2020	121	STATUS REPORT *(Joint) Regarding Rescheduling the Geofence Motion Hearing* by Okello T. Chatrie (Koenig, Laura) (Entered: 07/02/2020)
07/02/2020	123	MOTION for Issuance of Subpoenas *Duces Tecum and Memorandum in Support* by Okello T. Chatrie. (Attachments: # 1 Exhibit A)(Koenig, Laura) (Entered: 07/02/2020)
07/07/2020	126	Consent MOTION for Extension *of Supplemental Briefing Deadline On Magistrate Questions* by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 07/07/2020)

07/07/2020	127	ORDER as to Okello T. Chatrie. This matter comes before the Court on Defendant Okello T. Chatrie's Motion for Issuance of a Second Subpoena Duces Tecum Pursuant to Rule 17(c) (the "Second Motion for Subpoena"). The United States SHALL file a response to the Second Motion for Subpoena no later than July 13, 2020. It is SO ORDERED. Signed by District Judge M. Hannah Lauck on 7/7/2020. (sbea,) (Entered: 07/07/2020)
07/07/2020		Exhibit of DVD Received re 123 MOTION for Issuance of Subpoenas Duces Tecum and Memorandum in Support. Placed on shelf in Clerk's Office. (smej,) (Entered: 07/07/2020)
07/07/2020	128	ORDER − It is hereby ORDERED that the Defendant's Motion to Extend Supplemental Briefing on Magistrate Questions in this case is GRANTED. The parties must file any supplemental briefing on the issue by July 22, 2020. Signed by District Judge M. Hannah Lauck on 7/7/2020. (smej,) (Entered: 07/07/2020)
07/13/2020	129	RESPONSE by USA as to Okello T. Chatrie re 123 MOTION for Issuance of Subpoenas *Duces Tecum and Memorandum in Support*, 127 Order on Motion for Issuance of Subpoenas, (Attachments: # 1 Exhibit Subpoena Requests Updated to Include United States Additons)(Simon, Kenneth) (Entered: 07/13/2020)
07/16/2020	130	REPLY TO RESPONSE to by Okello T. Chatrie re 129 Response, 123 MOTION for Issuance of Subpoenas *Duces Tecum and Memorandum in Support* (Koenig, Laura) (Entered: 07/16/2020)
07/17/2020	131	ORDER that the Court GRANTS 123 Second Motion for Subpoena. See Order for details. Signed by District Judge M. Hannah Lauck on 7/17/2020. (jsmi,) (Main Document 131 replaced on 7/17/2020) (jsmi,). (Entered: 07/17/2020)
07/17/2020	132	ORDER re United States' standing argument raised in 129 response to Defendant Okello T. Chatrie's 123 Motion for Issuance of a Second Subpoena Duces Tecum. No later than July 31, 2020, Chatrie SHALL file a response to the United States' standing argument. This response SHALL NOT exceed 10 pages. If it so chooses, no later than August 7, 2020, the United States SHALL file a reply to Chatrie's response. This reply SHALL NOT exceed 10 pages. Signed by District Judge M. Hannah Lauck on 7/17/2020. (jsmi,) (Entered: 07/17/2020)
07/20/2020	133	Subpoena Issued as to Okello T. Chatrie. (Attachments: # 1 Exhibit A) (smej,) (Entered: 07/20/2020)
07/22/2020	134	RESPONSE by USA as to Okello T. Chatrie re 116 Order,, (Simon, Kenneth) (Entered: 07/22/2020)
07/22/2020	135	Supplemental Memorandum by Okello T. Chatrie re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C)(Koenig, Laura) (Entered: 07/22/2020)
07/29/2020	139	RESPONSE by USA as to Okello T. Chatrie re 135 Supplemental Memorandum (Simon, Kenneth) (Additional attachment(s) added on 7/30/2020: # 1 Appointment Order, # 2 Certificate, # 3 Oath of Office) (smej,). (Entered: 07/29/2020)
07/31/2020	140	RESPONSE by Google, LLC as to Okello T. Chatrie re 133 Subpoena(s) Issued (Amadi, Brittany) (Entered: 07/31/2020)
07/31/2020	141	MOTION for Leave to File *Documents Responsive to Rule 17(C) Subpoena Under Seal* by Google, LLC as to Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Amadi, Brittany) (Entered: 07/31/2020)
07/31/2020	142	ORDER as to Okello T. Chatrie. Having considered the motion of amicus curiae Google LLC for leave to file documents responsive to the July 22, 2020 subpoena under seal, and good cause appearing, it is hereby ORDERED that the motion is GRANTED. The clerk is DIRECTED to accept the documents lodged with the Court via e−mail for filing and to maintain them under seal. It is hereby ORDERED that Google will file a redacted version of the sealed documents on the public record within seven days of this Order.Signed by District Judge M. Hannah Lauck on 7/31/2020. (sbea,) (Entered: 07/31/2020)

07/31/2020	143	RESPONSE by Okello T. Chatrie re 129 Response, 132 Order,, (Koenig, Laura) (Entered: 07/31/2020)
08/07/2020	147	RESPONSE by Google, LLC as to Okello T. Chatrie re 133 Subpoena(s) Issued (Attachments: # 1 Exhibit A, # 2 Exhibit B)(Amadi, Brittany) (Entered: 08/07/2020)
08/19/2020	149	MOTION to Terminate Speedy Trial Hearing by Okello T. Chatrie. (Attachments: # 1 Envelope) (smej,) (Entered: 08/20/2020)
08/24/2020	151	ORDER − This matter comes before the Court on Defendant Okello T. Chatrie's pro se Motion to Terminate Speedy Trial Hearing, (the "Motion") 149 . The Court observes that Chatrie has legal representation through Laura Jill Koenig, Michael William Price, and Paul Geoffrey Gill. Despite having the benefit of Counsel, it appears that Chatrie filed this Motion without Counsels' legal assistance 149 . Because Chatrie remains represented by counsel, the Court DENIES WITHOUT PREJUDICE Chatrie's prose Motion to Terminate Speedy Trial Hearing 149 . Signed by District Judge M. Hannah Lauck on 8/24/2020. (smej,) (Entered: 08/24/2020)
09/28/2020	152	NOTICE OF ATTORNEY APPEARANCE Donald Eldridge Jeffrey, III appearing for USA. (Jeffrey, Donald) (Entered: 09/28/2020)
10/05/2020	153	ORDER − This matter comes before the Court on Defendant Okello T. Chatrie's Motion to Suppress Evidence Obtained from the Geo fence Warrant (the "Motion"). (ECF No. 29.) Upon review of the Parties' briefing on the Motion, the Court ORDERS the Parties to appear, in person, for a hearing on the Motion on Tuesday, November 17, 2020, at 10:00 a.m. Signed by District Judge M. Hannah Lauck on 10/05/2020. (tjoh,) (Entered: 10/05/2020)
10/05/2020		Set/Reset Deadlines re Motion or Report and Recommendation in case as to Okello T. Chatrie 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*, 21 MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search*, 20 MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search*, 18 MOTION to Suppress *Evidence Obtained from Willis Street Search*, 19 MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search*. Motion Hearing set for 11/17/2020 at 10:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 10/05/2020)
10/08/2020		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 10/22/2020 at 12:30 PM in Richmond Remote before District Judge M. Hannah Lauck. (khan,) (Entered: 10/08/2020)
10/16/2020	154	ORDER − The Parties clearly exchanged some information, such as Magistrate Bishop's educational history, either before or after the Subpoena was served. After reviewing the materials before it and in the interest of judicial efficiency, the Court DIRECTS the Parties to meet and confer about a potential stipulation of the below facts prior to the status conference with the Court scheduled for Thursday October 22, 2020. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 10/16/2020. (smej,) (Entered: 10/16/2020)
10/22/2020		Minute Entry for proceedings held before District Judge M. Hannah Lauck:Telephone Conference held via ZOOM as to Okello T. Chatrie held on 10/22/2020. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 10/22/2020)
10/22/2020	156	STIPULATION by Okello T. Chatrie *of Partial Facts Relating to Magistrate Issue* (Koenig, Laura) (Entered: 10/22/2020)
10/26/2020	157	TRANSCRIPT of Status Conference held on October 22, 2020, before Judge M. Hannah Lauck. Court reporter Diane Daffron, Telephone number 804−916−2893. **NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 11/25/2020. Redacted Transcript Deadline set for 12/28/2020. Release of Transcript Restriction set for 1/25/2021.(daffron, diane) (Entered: 10/26/2020)**

10/26/2020	160	ORDER − This matter comes before the Court on Magistrate David M. Bishop's Motion to Quash (the "Motion"). (ECF No. 145.) On October 22, 2019, Defendant Okello T. Chatrie moved this Court to suppress evidence, (the "Motion to Suppress"), that law enforcement officers obtained pursuant to a warrant of Chatrie's Google accounts ("the June 14, 2019 Geofence Warrant"). (Mot. Suppress Evid. 1, ECF No. 20.). The Court GRANTS the Motion to Quash. (ECF No. 145.) SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 10/26/2020. (smej,) (Entered: 10/26/2020)
11/09/2020	161	MOTION for Leave to Present Remote Testimony by Google, LLC as to Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Amadi, Brittany) (Entered: 11/09/2020)
11/09/2020	162	*Motion to Suppress Hearing* WITNESS LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 11/09/2020)
11/09/2020	163	*Motion to Suppress Hearing* EXHIBIT LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 11/09/2020)
11/09/2020	164	*11−17−20 Hearing* WITNESS LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 11/09/2020)
11/09/2020	165	*11−17−20 Hearing* EXHIBIT LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 11/09/2020)
11/11/2020	166	RESPONSE in Opposition by Okello T. Chatrie re 161 MOTION for Leave to Present Remote Testimony (Koenig, Laura) (Entered: 11/11/2020)
11/12/2020	167	REPLY TO RESPONSE to Google, LLC as to Okello T. Chatrie re 161 MOTION for Leave to Present Remote Testimony (Amadi, Brittany) (Entered: 11/12/2020)
11/12/2020		Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 11/12/2020 via ZOOM (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 11/16/2020)
11/16/2020	168	MOTION to Continue *November 17, 2020, Hearing* by Okello T. Chatrie. (Koenig, Laura) (Entered: 11/16/2020)
11/20/2020	169	STATUS REPORT *(Joint) on Potential Google Objections* by Okello T. Chatrie (Koenig, Laura) (Entered: 11/20/2020)
12/18/2020	170	ORDER − This matter comes before the Court on Defendant Okello T. Chatrie's Motion to Continue the November 17, 2020 Hearing (the "Motion"'), (ECF No. 168.) Upon review of the Parties' briefing on Chatrie's Motion to Suppress Evidence Obtained from the Geofence Warrant, the Court GRANTS the Motion, (ECF No. 168), and ORDERS the Parties to appear, in person, for a hearing on the Motion to Suppress Evidence on **Thursday, March 4, 2021, at 9:30 a.m.** in Courtroom 6100 of the Spottswood W. Robinson III and Robert R. Merhige, Jr. United States Courthouse. Signed by District Judge M. Hannah Lauck on 12/18/2020. (smej,) (Entered: 12/18/2020)
12/18/2020		Set/Reset Deadlines re Motion or Report and Recommendation in case as to Okello T. Chatrie 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*. Motion Hearing set for 3/4/2021 at 09:30 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 12/18/2020)
01/08/2021	171	**DISREGARD** − Letter from Brittany Amadi regarding the withdrawal of Alex Hemmer on behalf of Google LLC, (Amadi, Brittany) Modified on 1/12/2021 (smej,). (Entered: 01/08/2021)
01/11/2021		Notice of Correction re 171 Letter: The clerk has notified the filing attorney of the proper filing procedures for withdrawing from a case. The filing attorney has been instructed to file a motion to withdraw using the correct docket event. (smej,) (Entered: 01/11/2021)
01/14/2021	172	MOTION to Withdraw as Attorney by Alex Hemmer. by Google, LLC as to Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Amadi, Brittany) (Entered: 01/14/2021)
01/14/2021	173	Letter from Brittany Amadi (Amadi, Brittany) (Entered: 01/14/2021)

01/19/2021	174	ORDER − ORDER GRANTING MOTION TO WITHDRAW AS COUNSEL − Having considered the motion for leave to withdraw Alex Hemmer as counsel, and good cause appearing, it is hereby ORDERED that the that the motion is GRANTED. Signed by District Judge M. Hannah Lauck on 1/19/2021. (smej,) (Entered: 01/19/2021)
01/25/2021	175	MOTION to Compel *Disclosure of Expert Report and Exhibit 12 on or before February 5, 2021* by USA as to Okello T. Chatrie. (Attachments: # 1 Proposed Order Proposed Order)(Simon, Kenneth) (Entered: 01/25/2021)
02/03/2021	176	ORDER that the Court ORDERED Chatrie to respond to the Motion no later that Thursday, February 4, 2021 at noon. The Parties shall be advised of their duties under the Eastern District of Virginia Local Rule 37(H). The parties shall appear via teleconference on Thursday, February 4, 2021 at 2:00 p.m. for a status conference in this matter. Signed by District Judge M. Hannah Lauck on 2/3/21. (khan,) (Entered: 02/03/2021)
02/03/2021		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 2/4/2021 at 02:00 PM in Richmond Remote before District Judge M. Hannah Lauck. (khan,) (Entered: 02/03/2021)
02/03/2021	177	RESPONSE to Motion by Okello T. Chatrie re 175 MOTION to Compel *Disclosure of Expert Report and Exhibit 12 on or before February 5, 2021* (Koenig, Laura) (Entered: 02/03/2021)
02/04/2021	178	Letter from Brittany Amadi regarding Witness Availability, (Amadi, Brittany) (Entered: 02/04/2021)
02/04/2021	179	ORDER that the Court denies as moot 175 Motion to Compel. The Court ORDERS that the Parties submit expert reports no later than February 16, 2021. The Parties SHALL file any arguments as to an extension to the February 16, 2021, deadline no later than February 12, 2021. On February 25, 2021, the Parties SHALL file their updated witness and exhibit lists and provide the Court with two courtesy copies of the exhibits, should they conform to paper copies. Signed by District Judge M. Hannah Lauck on 2/4/2021. (jsmi,) (Entered: 02/04/2021)
02/05/2021	181	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 2/5/2021 (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 02/05/2021)
02/11/2021	184	Letter from Catherine Carroll (Carroll, Catherine) (Entered: 02/11/2021)
02/22/2021	185	ORDER as to Okello T. Chatrie. In light of the quickly approaching hearing on the pending Motion to Suppress Evidence Obtained from Chatrie's Google Accounts, (ECF No. 20), Counsel for Chatrie SHALL file on February 25, 2021, a status update regarding Chatries ability to personally appear at the hearing currently scheduled for March 45, 2021. On February 26, 2021, at 1:30 p.m., the Parties SHALL appear before the Court, via video teleconference, for a status conference. It is SO ORDERED. Signed by District Judge M. Hannah Lauck on 2/22/2021. (sbea,) (Entered: 02/22/2021)
02/22/2021		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 2/26/2021 at 01:30 PM in Richmond Remote before District Judge M. Hannah Lauck. (khan,) (Entered: 02/22/2021)
02/22/2021		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 2/25/2021 at 04:00 PM in Richmond Remote before District Judge M. Hannah Lauck. (khan,) (Entered: 02/22/2021)
02/25/2021	186	*Motion to Suppress 3−4−21 Hearing* WITNESS LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 02/25/2021)
02/25/2021	187	*Motion to Suppress Hearing* EXHIBIT LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 02/25/2021)
02/25/2021	188	RESPONSE by Okello T. Chatrie re 185 Order,, (Gill, Paul) (Entered: 02/25/2021)
02/25/2021	189	EXHIBIT LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 02/25/2021)

02/25/2021	190	WITNESS LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 02/25/2021)
02/25/2021		Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 2/25/2021 (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 02/26/2021)
02/26/2021	191	ORDER − This matter comes before the Court sua sponte. On February 25, 2021, the Court held a status conference in this matter over Zoom. For the reasons stated from the Bench, the Court ORDERS the Parties to file no later than Friday, February 26, 2021, at 1:00 p.m., their positions on COVID−19 protocol and procedures required by applicable governmental and health agencies for an in−person hearing on March 4, 2021. The Parties SHALL appear before the Court via video teleconference for a status conference in this matter on Friday, February 26, 2021, at 4:30 p.m. Signed by District Judge M. Hannah Lauck on 02/26/2021. (tjoh,) (Entered: 02/26/2021)
02/26/2021		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 2/26/2021 at 04:30 PM in Richmond Remote before District Judge M. Hannah Lauck. (khan,) (Entered: 02/26/2021)
02/26/2021	192	Letter from Catherine Carroll (Carroll, Catherine) (Entered: 02/26/2021)
02/26/2021	193	Position on *Defendant's Presence at Suppression Hearing Following COVID−19 Diagnosis* by USA as to Okello T. Chatrie *Defendant's Presence at Suppression Hearing Following COVID−19 Diagnosis* (Simon, Kenneth) (Entered: 02/26/2021)
02/26/2021	194	RESPONSE by Okello T. Chatrie re 191 Order,, *Position on COVID−19 protocol and procedures* (Gill, Paul) (Entered: 02/26/2021)
02/26/2021		Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 2/26/2021 (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 03/01/2021)
03/04/2021		Set/Reset Deadlines re Motion or Report and Recommendation in case as to Okello T. Chatrie 20 MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search*. Motion Hearing set for 3/5/2021 at 09:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 03/04/2021)
03/04/2021	198	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Motion Hearing as to Okello T. Chatrie held on 3/4/2021 re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* filed by Okello T. Chatrie. Dft adduced evidence. Motion hearing continued to March 6, 2021 at 9:00 a.m. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) Modified on 3/8/2021 (khan,). (Entered: 03/08/2021)
03/05/2021	199	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Motion Hearing as to Okello T. Chatrie held on 3/5/2021 re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* filed by Okello T. Chatrie. Dft adduced evidence, rested. Govt adduced evidence, rested. Briefing schedule set. Govt. maintained a set of exhibits for chambers use. Parties to maintain official set for record. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 03/08/2021)
03/09/2021	200	ORDER as to Okello T. Chatrie − For the reasons stated from the Bench, Defendant Okello T. Chatrie SHALL file supplemental briefing on the Geofence Motion to Suppress no later than April 30, 2021. On or before May 21, 2021, the United States SHALL file its response. On or before June 4, 2021, Chatrie SHALL file his reply. The Court ORDERS the Parties to appear for a hearing on all outstanding matters on **June 24, 2021, at 10:00 a.m.** The Court DENIES as moot Google's Motion for Leave to Present Remote Testimony. (ECF No. 161.) Signed by District Judge M. Hannah Lauck on 3/9/2021. (smej,) (Entered: 03/09/2021)
03/09/2021		Set Motion in case as to Okello T. Chatrie. Motion Hearing set for 6/24/2021 at 10:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 03/09/2021)
03/29/2021	201	TRANSCRIPT of Motion to Suppress held on March 4, 2021, before Judge M. Hannah Lauck. Court reporter Diane Daffron, Telephone number 804−916−2893.

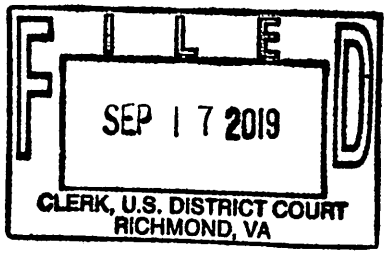
		NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 4/28/2021. Redacted Transcript Deadline set for 6/1/2021. Release of Transcript Restriction set for 6/28/2021.(daffron, diane) (Entered: 03/29/2021)
03/29/2021	202	TRANSCRIPT of Motion to Suppress (Day 2) held on March 5, 2021, before Judge M. Hannah Lauck. Court reporter Diane Daffron, Telephone number 804−916−2893. **NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 4/28/2021. Redacted Transcript Deadline set for 6/1/2021. Release of Transcript Restriction set for 6/28/2021.(daffron, diane) (Main Document 202 replaced on 4/29/2021) (tjoh,). (Entered: 03/29/2021)**
04/30/2021	203	MOTION for Leave to File *Brief Exceeding 30 Pages* by Okello T. Chatrie. (Attachments: # 1 Exhibit 1, # 2 Proposed Order)(Koenig, Laura) (Entered: 04/30/2021)
05/03/2021	204	ORDER − Upon motion of defense counsel, with good cause having been shown, it is hereby ORDERED that the Defendants Motion for Leave to File Brief Exceeding 30 Pages in this case is GRANTED. (ECF No. 203.) Mr. Chatries Post−Hearing Brief on Geofence General Warrant is deemed timely filed. Mr. Chatrie shall refile that brief as a separate docket entry within three business days of this Order. Signed by District Judge M. Hannah Lauck on 5/3/2021. (smej,) (Entered: 05/03/2021)
05/03/2021	205	Supplemental Memorandum by Okello T. Chatrie re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* (Koenig, Laura) (Entered: 05/03/2021)
05/14/2021	206	MOTION for Bond by Okello T. Chatrie. (Gill, Paul) (Entered: 05/14/2021)
05/21/2021	207	MOTION for Leave to File *Post−Hearing Supplemental Response in Opposition* by USA as to Okello T. Chatrie. (Attachments: # 1 Proposed Order Proposed Order, # 2 Exhibit Response in Opposition Post−Hearing Supplemental Brief)(Simon, Kenneth) (Entered: 05/21/2021)
05/24/2021	208	ORDER − Upon Motion of the United States of America, by and through attorneys, Raj Parekh, Acting United States Attorney for the Eastern District of Virginia, Kenneth R. Simon, Jr., and Peter S. Duffey, Assistant United States Attorneys, for leave to file an omnibus responsive brief that is in excess of thirty pages pursuant to Local Criminal Rule 47(F)(3). For good cause shown, the Court GRANTS the United States motion. Accordingly, the United States may file its omnibus responsive brief that is in excess of thirty pages. Signed by District Judge M. Hannah Lauck on 5/24/2021. (smej,) (Entered: 05/24/2021)
05/30/2021	209	RESPONSE in Opposition by USA as to Okello T. Chatrie re 206 MOTION for Bond (Attachments: # 1 Exhibit Still Photos from Robbery Video)(Simon, Kenneth) (Entered: 05/30/2021)
06/02/2021		Set as to Okello T. Chatrie: Bond Reconsideration Hearing set for 6/3/2021 at 2:15 PM in Richmond Courtroom 5400 before Magistrate Judge Elizabeth W. Hanes. (mful) (Entered: 06/02/2021)
06/03/2021	210	Addendum to Pretrial Services Bond Report (Sealed Document) as to Okello T. Chatrie (taylor, sheree) (Entered: 06/03/2021)

06/03/2021	211	Minute Entry for proceedings held before Magistrate Judge Elizabeth W. Hanes: Bond Reconsideration Hearing as to Okello T. Chatrie held on 6/3/2021; Deft adduced evidence; Arguments heard; Findings stated from the bench; Motion denied; Order to follow; Deft remanded. (FTR)(mful) (Entered: 06/04/2021)
06/03/2021	212	ORDER denying 206 Motion for Bond as to Okello T. Chatrie. Signed by Magistrate Judge Elizabeth W. Hanes on 6/3/21. (mful) (Entered: 06/04/2021)
06/04/2021	213	REPLY TO RESPONSE to by Okello T. Chatrie re 209 Response in Opposition (Koenig, Laura) (Entered: 06/04/2021)
06/17/2021	214	RESPONSE by USA as to Okello T. Chatrie re 205 Supplemental Memorandum (Simon, Kenneth) (Entered: 06/17/2021)
06/24/2021	215	Minute Entry for proceedings held before District Judge M. Hannah Lauck (Daffron, OCR): Matter came on for hearing as to Okello T. Chatrie on 6/24/2021 re: supplemental briefing to 29 Motion to Suppress Evidence Obtained from a "Geofence" General Warrant filed by Okello T. Chatrie. Defense counsel heard. Government heard. Matter taken under advisement by the Court. Defendant remanded to custody (rpiz) (Entered: 06/25/2021)
06/30/2021	216	NOTICE *of Supplemental Authority* by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 06/30/2021)
07/15/2021	217	TRANSCRIPT of argument on summary judgment motion Proceedings held on June 24, 2021, before Judge M. Hannah Lauck. Court reporter Diane Daffron, Telephone number 804−916−2893. **NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 8/16/2021. Redacted Transcript Deadline set for 9/14/2021. Release of Transcript Restriction set for 10/13/2021.(daffron, diane) (Entered: 07/15/2021)**
07/16/2021	218	RESPONSE by Okello T. Chatrie re 216 Notice (Other) (Koenig, Laura) (Entered: 07/16/2021)
12/16/2021	219	NOTICE *of Supplemental Authority* by Okello T. Chatrie re 104 Supplemental Memorandum, 205 Supplemental Memorandum, 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* (Attachments: # 1 Exhibit A)(Koenig, Laura) (Entered: 12/16/2021)
03/03/2022	220	MEMORANDUM OPINION as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 3/3/22. (khan,) (Entered: 03/03/2022)
03/03/2022	221	ORDER denying 29 Motion to Suppress as to Okello T. Chatrie (1). Signed by District Judge M. Hannah Lauck on 3/3/22. (khan,) (khan,). (Entered: 03/03/2022)
03/03/2022	222	Sealed Document signed by M. Hannah Lauck, U.S. District Judge on 3/3/22. (khan,) (Entered: 03/03/2022)
03/03/2022	223	ORDER denying 18 Motion to Suppress as to Okello T. Chatrie (1); denying 19 Motion to Suppress as to Okello T. Chatrie (1); denying 20 Motion to Suppress as to Okello T. Chatrie (1); denying 21 Motion to Suppress as to Okello T. Chatrie (1). Signed by District Judge M. Hannah Lauck on 3/3/22. (khan,) (Entered: 03/03/2022)
05/02/2022		Set/Reset Hearings as to Okello T. Chatrie: Plea Agreement Hearing set for 5/9/2022 at 02:30 PM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 05/02/2022)
05/06/2022	224	CRIMINAL INFORMATION as to Okello T. Chatrie (1) count(s) 1s, 2s. (jpow,) (Entered: 05/06/2022)
05/09/2022	226	Minute Entry for proceedings held before District Judge M. Hannah Lauck (Court Reporter Daffron, OCR): Plea Agreement Hearing as to Okello T. Chatrie held on 5/9/2022. Waiver of Indictment, Plea Agreement, and Statement of Facts filed in open

		court. Plea entered by Okello T. Chatrie (1) Guilty as to Counts 1s and 2s of the Criminal Information; Court accepted plea. Judgment: Defendant guilty as charged in Counts 1s and 2s. Sentencing set for 8/2/2022 at 11:00 AM. Defendant remanded to custody (rpiz) (Entered: 05/09/2022)
05/09/2022	227	WAIVER OF INDICTMENT by Okello T. Chatrie (rpiz) (Entered: 05/09/2022)
05/09/2022	228	PLEA AGREEMENT as to Okello T. Chatrie (rpiz) (Entered: 05/09/2022)
05/09/2022	229	STATEMENT OF FACTS as to Okello T. Chatrie (rpiz) (Entered: 05/09/2022)
05/09/2022	230	Order for sentencing guidelines as to Okello T. Chatrie: Sentencing set for 8/2/2022 at 11:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck (signed by District Judge M. Hannah Lauck on 5/9/2022) (rpiz) (Entered: 05/09/2022)
05/09/2022	231	CONSENT ORDER OF FORFEITURE as to Okello T. Chatrie (signed by District Judge M. Hannah Lauck on 5/9/2022) (rpiz) (Entered: 05/09/2022)
06/28/2022	232	PRESENTENCE INVESTIGATION REPORT (Disclosed Presentence Investigation Report) (SEALED − government and defense counsel) as to Okello T. Chatrie. Objections to PSI due 07/12/2022. (Harrison, Dorothy) (Entered: 06/28/2022)
07/08/2022		Set/Reset Hearings as to Okello T. Chatrie: Sentencing set for 8/10/2022 at 02:00 PM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 07/08/2022)
07/27/2022	233	PRESENTENCE INVESTIGATION REPORT (Sentencing Presentence Investigation Report) (SEALED − government and defense counsel) as to Okello T. Chatrie. (Harrison, Dorothy)INCLUDES ADDENDUM (Entered: 07/27/2022)
07/27/2022	235	Position on Sentencing by Okello T. Chatrie (Attachments: # 1 Exhibit B, # 2 Exhibit C)(Koenig, Laura) (Additional attachment(s) added on 7/27/2022: # 3 Ex. A Under Seal) (khan,). (Entered: 07/27/2022)
07/27/2022	236	Position on Sentencing by USA as to Okello T. Chatrie (Attachments: # 1 Exhibit Still Images from Surveillance and Threatening Letter)(Simon, Kenneth) (Entered: 07/27/2022)
08/08/2022	237	PRESENTENCE INVESTIGATION REPORT WITH SECOND ADDENDUM AND VICTIM IMPACT STATEMENTS (Sentencing Presentence Investigation Report) (SEALED − government and defense counsel) as to Okello T. Chatrie. (Attachments: # 1 VICTIM IMPACT STATEMENT #1, # 2 VICTIM IMPACT STATEMENT #2)(smith, lisa) (Entered: 08/08/2022)
08/10/2022	238	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Sentencing held on 8/10/2022 for Okello T. Chatrie (1), Count(s) 1, 2, DISMISSED ON MOTION OF GOVT.; Count(s) 1s, 57 MONTHS IMPRISONMENT, 3 YEARS SUPERVISED RELEASE, $100 S/A, $196,932.01 RESTITUTION; Count(s) 2s, 84 MONTHS IMPRISONMENT TO BE SERVED CONSECUTIVE TO CT. 1, 3 YEARS SUPERVISED RELEASE TO BE SERVED CONCURRENT TO CT. 1, $100 S/A. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 08/10/2022)
08/19/2022	239	JUDGMENT as to Okello T. Chatrie (1), Count(s) 1, 2, DISMISSED ON MOTION OF GOVT.; Count(s) 1s, 57 MONTHS IMPRISONMENT, 3 YEARS SUPERVISED RELEASE, $100 S/A, $196,932.01 RESTITUTION; Count(s) 2s, 84 MONTHS IMPRISONMENT TO BE SERVED CONSECUTIVE TO CT. 1, 3 YEARS SUPERVISED RELEASE TO BE SERVED CONCURRENT TO CT. 1, $100 S/A. Signed by District Judge M. Hannah Lauck on 8/19/22. (khan,) (Entered: 08/19/2022)
08/19/2022	240	Sealed Statement of Reasons as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 8/19/22. (khan,) (Entered: 08/19/2022)
08/25/2022	241	NOTICE OF APPEAL by Okello T. Chatrie as to 239 Judgment, 220 Memorandum Opinion, 221 Order on Motion to Suppress (Koenig, Laura) (Entered: 08/25/2022)
08/26/2022	242	Transmission of Notice of Appeal to 4CCA as to Okello T. Chatrie to US Court of Appeals re 241 Notice of Appeal. (All case opening forms, plus the transcript guidelines, may be obtained from the Fourth Circuit's website at

		www.ca4.uscourts.gov) (jsmi,) (Main Document 242 replaced on 8/29/2022) (jpow,). (Entered: 08/26/2022)
08/29/2022		USCA Case Number 22−4489, Case Manager A. Walker, for 241 Notice of Appeal filed by Okello T. Chatrie. (smej,) (Entered: 08/29/2022)
08/29/2022	243	ORDER of USCA as to Okello T. Chatrie re 241 Notice of Appeal. The court appoints the Federal Defender for the Eastern District of Virginia to represent appellant in this case. (22−4489) (smej,) (Entered: 08/29/2022)
09/06/2022	244	NOTICE *of Publication and Finality of Consent Order of Forfeiture* by USA as to Okello T. Chatrie re 231 Consent Order for Forfeiture of Property (Attachments: # 1 Declaration of Publication)(Lee, Janet) (Entered: 09/06/2022)
09/12/2022	245	TRANSCRIPT REQUEST by Okello T. Chatrie for proceedings held on May 9, 2022 (change of plea hearing) before Judge Lauck, (Pratt, Frances) (Entered: 09/12/2022)
09/13/2022	246	Transcript Order Acknowledgment from USCA re 241 Notice of Appeal: Court Reporter/Transcriber Diane Daffron. (smej,) (Entered: 09/13/2022)
10/04/2022	247	TRANSCRIPT of proceedings as to Okello T. Chatrie for dates of May 9, 2022 before Judge M. Hannah Lauck, re 241 Notice of Appeal Court Reporter Diane Daffron, Telephone number 804−916−2893. **NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov** ***Does this satisfy all appellate orders for this reporter? y*** **Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 11/3/2022. Redacted Transcript Deadline set for 12/5/2022. Release of Transcript Restriction set for 1/2/2023.(daffron, diane) (Main Document 247 replaced at request of Court Reporter on 10/5/2022) (jsmi,). (Entered: 10/04/2022)**

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division



UNITED STATES OF AMERICA	)	No. 3:19CR130
	)	
v.	)	Count 1: 18 U.S.C. §§ 2113(a), (d), and (e)
	)	Forced Accompaniment During Armed
OKELLO T. CHATRIE,	)	Credit Union Robbery
	)	
Defendant.	)	Count 2: 18 U.S.C. § 924(c)(1)(A)
	)	Use, Carry, and Brandish a Firearm During
	)	and in Relation to a Crime of Violence
	)	
	)	Forfeiture Allegation

September 2019 Term – at Richmond, Virginia

INDICTMENT

THE GRAND JURY CHARGES THAT:

COUNT ONE
(Forced Accompaniment during an Armed Credit Union Robbery)

On or about May 20, 2019, in the Eastern District of Virginia, the defendant, OKELLO T. CHATRIE, by force and violence, and intimidation, did take from the person and presence of another, namely J.W. and K.C., employees of the Call Federal Credit Union located at 3640 Call Federal Drive, Midlothian, Virginia, 23112, approximately $195,000 in United States currency, belonging to, and in the care, custody, control, management and possession of the Call Federal Credit Union, the accounts of which were then insured by the National Credit Union Administration Board; and in committing such offense, the defendant did knowingly and unlawfully assault and put in jeopardy the life of other persons, namely Call Federal Credit Union employees and customers, by the use of a dangerous weapon, namely a firearm; and further, the

defendant, in committing this offense, did knowingly and unlawfully force another person to accompany him without the consent of such person.

(In violation of Title 18, United States Code, Sections 2113(a), 2113(d), and 2113(e)).

COUNT TWO

(Use, Carry, and Brandish a Firearm During and in Relation to a Crime of Violence)

On or about May 20, 2019, in the Eastern District of Virginia, the defendant, OKELLO T. CHATRIE, did knowingly and unlawfully use, carry, and brandish a firearm during and in relation to a crime of violence for which he may be prosecuted in a court of the United States, that is, forced accompaniment during an armed credit union robbery, as charged in Count One of this Indictment, which is re-alleged as if fully set forth here.

(In violation of Title 18, United States Code, Sections 924(c)(1)(A)(i) and (ii)).

FORFEITURE ALLEGATION

Pursuant to Federal Rule of Criminal Procedure 32.2, the defendant, OKELLO T. CHATRIE, is notified that if convicted of Count One of this Indictment, the defendant shall forfeit to the United States, any property, real or personal, which constitutes or is derived from proceeds traceable to such violation.

This property includes, but is not limited to:

A sum of money of at least $195,000, which represents the total proceeds of the offense charged, to be partially offset by $102,293 seized from 1317 Willis Street, Richmond, Virginia, 23224 on August 13, 2019.

If the property subject to forfeiture cannot be located, the United States will seek an order forfeiting substitute assets.

The defendant is further notified that upon conviction of the offenses alleged in Count One or Count Two of this Indictment, the defendant shall forfeit any firearms and ammunition involved in or used in any knowing violation of such offenses.

Property subject to forfeiture includes, but is not limited to:

A 9 mm Taurus G2C pistol, serial number TLW87541; and

all accompanying ammunition.

(In accordance with Title 18, United States Code, Sections 924(d) and 981(a)(1)(C) as incorporated by Title 28, United States Code, Section 2461(c)).

A TRUE BILL:

FOREPERSON

G. ZACHARY TERWILLIGER
United States Attorney

Pursuant to the E-Government Act, the original of this page has been filed under seal in the Clerk's Office

By:
Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA	)	
	)	
	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

DEFENDANT OKELLO CHATRIE'S MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A "GEOFENCE" GENERAL WARRANT

Okello Chatrie, through counsel, moves the Court to suppress evidence that law enforcement obtained pursuant to a warrant authorizing state police to obtain the cell phone location information of 19 Google users who happened to be in the vicinity of a bank robbery on a Monday afternoon in Richmond. This is a "geofence" warrant, and it is an unlawful and unconstitutional general warrant that is both overbroad and lacks the particularity required by the Fourth Amendment. The Court should therefore suppress all evidence obtained from the warrant and all fruit of the poisonous tree, including the identification of Mr. Chatrie.

INTRODUCTION

Law enforcement obtained Mr. Chatrie's cell phone location information from Google using a "geofence" warrant. A geofence warrant requires Google to produce data regarding all devices using Google services within a geographic area during a given window of time. But unlike a typical warrant for location data, this geofence warrant did not identify Mr. Chatrie in any way. In fact, it did not identify any of the 19 people whose personal information was searched by the Virginia state police as a result. Instead, the warrant operated in reverse: it required Google to identify a large cache of deeply private data—held in the "Sensorvault"—and then allowed police

the discretion to obtain private information from devices of interest. This is nothing less than the modern-day incarnation of a "general warrant," and it is prohibited by the Fourth Amendment.

Virginia police obtained a warrant for the Sensorvault data in this case, presumably because they recognized, correctly, that such information is intensely private and constitutionally protected. Like the cell site location information ("CSLI") in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), cell phone users constantly generate Sensorvault location information by either (1) using devices running Google's software ("Android" phones), or (2) interacting with Google services (Maps, Gmail, Search, YouTube, etc.). *See* Background, *infra*. And as in *Carpenter*, users have a reasonable expectation of privacy in their location data, which is sensitive and revealing of the "privacies of life." 138 S. Ct. at 2214. Not only can this data reveal private activities in daily life, but it can also show that someone is inside a constitutionally protected space, such as a home, church, or hotel—all of which are in the immediate vicinity of the bank that was robbed in Richmond. The ability to access data that can locate individuals quickly, cheaply, and retroactively is an unprecedented expansion of law enforcement power, and doing so constitutes a Fourth Amendment search, just as it did in *Carpenter*. *Id* at 2230; *see also Prince Jones v. United States*, 168 A.3d 703, 712 (D.C. 2017) (recognizing that access to cell phone location data permits the "police to locate a person whose whereabouts were previously completely unknown."). In fact, the location data available in Google's Sensorvault is even more precise than the data in *Carpenter*. Google can pinpoint an individual's location to approximately 20 meters compared to "a few thousand meters" for cell site location data. Google, *Find and Improve Your Location's Accuracy* (Oct. 24, 2019), https://support.google.com/maps/answer/2839911?co=GENIE.Platform%3DAndroid&oco=1. Therefore, the third-party doctrine should not apply, and a valid warrant should be required for law enforcement to access any user's Sensorvault data.

Nonetheless, the fact that law enforcement obtained a warrant in this case does not save the search from constitutional infirmity. This is no ordinary warrant. It is a general warrant purporting to authorize a classic dragnet search of every Google user who happened to be near a bank in suburban Richmond during rush hour on a Monday evening. This is the kind of investigatory tactic that the Fourth Amendment was designed to guard against. Geofence warrants like the one in this case are incapable of satisfying the probable cause and particularity requirements, making them unconstitutional general warrants.

In the alternative, should the Court find that geofence warrants are not wholly impermissible under the Fourth Amendment, the warrant in this case fails to satisfy the particularity requirement and fails to establish probable cause to search Mr. Chatrie's Sensorvault data. Despite the prevalence of Google phones and services, there are no facts to indicate that the bank robber used either, whether ever or at the time of the robbery. There is no evidence that the robber used an Android operating system or accessed any Google service in connection with the crime. Instead, based only on Google's popularity and the prevalence of cell phones generally, law enforcement searched a trove of private location information belonging to 19 unknown Google users who happened to be near a local bank on a Monday evening. The government's generalized assumptions about cell phone use, devoid of any specific factual nexus to the criminal activities alleged, are insufficient to establish probable cause for the sweeping and invasive search in this case. Additionally, the discretion afforded to police to determine which accounts to search is the essence of an unparticularized warrant. In short, the warrant both lacks particularity and is fatally overbroad.

Finally, the good faith exception to the exclusionary rule does not apply to evidence obtained from this warrant. Given the lack of particularity and absence of probable cause for any

and all individuals whose data would be searched, no objectively reasonable officer could rely on such a warrant. For these reasons, the Court must suppress all evidence obtained from the geofence warrant and all fruit of the poisonous tree.

BACKGROUND

Over the last few decades, the ability of law enforcement to cheaply and easily access highly sensitive digital data has progressed in leaps and bounds. Requests for user information from cellular service providers and other online service providers like Google have become a powerful investigative tool for law enforcement to locate and identify almost any individual, as 96% of Americans now own cell phones. Pew Research Center, *Mobile Fact Sheet* (Jun. 12, 2019), http://www.pewinternet.org/fact-sheet/mobile/. As a result, "[o]nly the few without cell phones could escape this tireless and absolute surveillance." *Carpenter*, 138 S. Ct. at 2218.

Law enforcement can locate cell phones using user location data, which is collected and maintained by cell phone companies as well as third-party service providers, such as Google. For example, Google regularly collects detailed location information from all phones running Google's "Android" operating system. Android phones routinely transmit their GPS location to Google, but Google can also identify a phone's location based on nearby Wi-Fi networks, mobile networks, and device sensors. Google, *How Google Uses Location Information* (Oct. 25, 2019), https://policies.google.com/technologies/location-data. While it is possible to turn off location history on an Android phone, opening Google Maps or running a Google search will still pinpoint a user's latitude and longitude and create a record with Google. Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb (identifying Google services that register a user's application upon use, including "Location History, Web and App activity, and …

device-level Location Services."). Even non-Android devices, such as Apple iPhones, transmit location information to Google when individuals use a Google service or application, such as Gmail, Search, and Maps. *Id.* Consequently, although Google's Sensorvault does not collect data on every phone, it nevertheless contains an enormous trove of location information on most Android phones and many iPhones in use in the United States.

In recent years, law enforcement has begun requesting this data from Google using geofence warrants to identify devices present in a geographic area during a window of time. Jennifer Valentino-DeVires, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html. Since a geofence warrant identifies a geographic area, and not a suspect, these requests "ensnare anyone who uses Google services at specific times in the . . . areas [near a crime]," sweeping up innocent individuals in an unconstitutional dragnet search. Debra Cassens Weiss, *FBI Asks Google to Turn Over All Data on Users Who Were Close to Robbery Locations*, ABA Journal (Oct. 25, 2018), http://www.abajournal.com/news/article/fbi_asks_google_for_location_data_on_anyone_close_to_robbery_locations_in_t. Individuals may be caught up in this search by merely using an Android phone, conducting an internet search using Google, running a Google application such as Google Maps or YouTube, or even receiving an automatic weather update from an Android service. Nakashima, *supra*, *Google Tracks Your Movements, Like it or Not*.

FACTS

Geofence warrants compel Google to produce location information about devices interacting with Google technology within a geographic area during a given timeframe. In this case, the government requested data from Google regarding all Google devices that were within 150 meters of the Call Federal Credit Union in Richmond, Virginia, during a one-hour period at

the beginning of Monday evening rush hour. Specifically, the warrant sought information on all devices within 150 meters of 37° 26' 18.3" N, 77° 35' 16.4" W between 4:20 and 5:20 p.m. EST. *See* Ex. A State Warrant at 3[1]. In addition to a major thoroughfare (U.S. Route 360), the immediate area includes a Ruby Tuesday restaurant, a Hampton Inn hotel, a mini storage facility, an apartment complex for seniors, another residential apartment complex, and the Journey Christian Church, a very large[2] church located directly across from the Credit Union. The 150-meter radius encompasses both the bank and the church as well as their parking lots.

The warrant describes a three-step process. First, Google provided "anonymized information" about all Google users in the area between 4:20 and 5:20 p.m., including "a numerical identifier for the account, the type of account, time stamped location coordinates and the data source." *See* Ex. A (State Warrant) at 2. This initial search affected 19 unique Google users, yielding 209 location points over an hour. *See* Ex. B (Excel Sheet 1). Law enforcement then reviewed the data and attempted to "narrow down the list" based on other known information. *See* Ex. A (State Warrant) at 2. Next, in a private letter to Google without any additional judicial scrutiny, police requested additional "contextual data points with points of travel *outside* of the [geofence]" and for "30 minutes before AND 30 minutes after the initial search time periods" for a subset of 9 users. *Id*. (emphasis added). This produced 680 location points over a total of two hours. *See* Ex. C (Excel Sheet 2). Finally, police returned to Google once again to obtain

[1] The government has provided the defense with a sealed copy of this search warrant with no explanation as to why it remains sealed. Per the Chesterfield County Circuit Court Clerk's Office, this warrant and its supporting documents will remain sealed absent further intervention from the government until December 19, 2019. Because the document is and will remain sealed until further action by the government, Mr. Chatrie does not attach it here, but refers to it for when the Court is able to review a copy.

[2] In 2017, Outreach Magazine, which tracks church attendance and congregation growth rates, reported that Journey Christian Church had 1,743 people attend its church and ranked as one of the fastest-growing congregations in the country. Outreach Magazine, Journey Christian Church, https://outreach100.com/churches/journey-christian-church.

"identifying account information/CSI" for 3 users, including: usernames, subscriber information, as well as all email addresses, electronic devices, and phone numbers associated with the accounts.[3] *See* Ex. A (State Warrant) at 3.

ARGUMENT

The acquisition of Mr. Chatrie's data from Google was a Fourth Amendment search. In either event, the action intruded upon Mr. Chatrie's reasonable expectation of privacy in his location data. This is critical because the warrant obtained by Virginia police is invalid. It is a general warrant, irredeemably unreasonable and completely impermissible under the Fourth Amendment. Law enforcement simply cannot establish the requisite probable cause and particularity to search a trove of data belonging individuals suspected of no wrongdoing. As a result, the warrant is also fatally overbroad and lacking particularity. Such a warrant is void from its inception and is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law.").

I. The Acquisition of Mr. Chatrie's Data from Google Was a Fourth Amendment Search.

In *Carpenter*, the Supreme Court held that individuals have a reasonable expectation of privacy in their cell phone location data, and that the government's acquisition of those records in that case was a Fourth Amendment search. 138 S. Ct. at 2217. This holding applies with equal force in the context of a location data request directed to Google, which involves information that is more precise than the data at issue in *Carpenter*. Regardless of whether the Court analyzes this

[3] The warrant does not define "CSI" at any point in the warrant or application.

claim under the reasonable expectation of privacy framework set forth in *Katz* or a property-based theory, it should reach the conclusion that acquisition of Defendant's location information constituted a Fourth Amendment search.

A. Cell Phone Users Have a Reasonable Expectation of Privacy in Their Location Information.

In considering whether individuals reasonably expect information to remain private, the Supreme Court has crafted "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also Carpenter*, 138 S. Ct. at 2219 (applying the *Katz* analysis in the context of historical cell site location information and concluding that users have a reasonable expectation of privacy in this information). Cell phone location information is highly sensitive, as shown by the watershed decision in *Carpenter*, and this classification applies to Google's Sensorvault location data based on the strong similarities between the two types of information. In the majority opinion, Justice Roberts emphasized the revealing nature of historical cell site location information and compared this quality to that of GPS location information. *Id.* at 2217. ("*As with GPS information*, the time-stamped data provides an intimate window into a person's life, revealing … his particular movements" (citation omitted) (emphasis added)). GPS is one of the primary methods that Google uses to compile Sensorvault location data. Google, *supra*, *How Google Uses Location Information*. Google also includes location data from mobile networks, *id.*, the same technology at issue in *Carpenter*.

The fact that Google, a third-party service provider, collects and maintains this location information does not diminish an individual's expectation of privacy in it. *Carpenter*, 138 S. Ct. at 2220. While the third-party doctrine stands for the general proposition that an individual has a

reduced expectation of privacy in information knowingly shared with another, the rule is not to be "mechanically" applied in the digital age. *Id.* at 2219. To do so would "[fail] to contend with the seismic shifts in digital technology that made possible the tracking of not only [Mr. Chatrie's] location but also everyone else's, not for a short period but for years and years." *Id.* Indeed, Google is no ordinary third party: "Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible." *Id*. The fact that Google is able to provide location data information for a given place and time in the past is possible only because of its exhaustive and constant collection of user data.

In *Carpenter*, the Court rejected the government's contention that the third-party doctrine applied to historical cell-site information, and this holding applies to cell phone location data acquired through Google. The Court provided two main rationales for its decision: cell-site location information is qualitatively different from types of business records to which the doctrine may apply based on its revealing nature, and users do not voluntarily share their cell-site location information with their service provider. 138 S. Ct. at 2219–20. These two rationales apply with equal force to the location information Google stores, and as such third-party doctrine is inapposite to data gleaned from Google under the warrant.

Google location records are qualitatively different from the business records to which the third-party doctrine traditionally applies. *See Smith v. Maryland*, 442 U.S. 735, 742 (numbers dialed on a landline); *United States v. Miller*, 425 U.S. 435, 440 (1976) (bank deposit slips). Instead, they reveal the same type of information as the cell-site location data considered private in *Carpenter*, and they do so in an even more precise manner. Google, *supra*, *Find and Improve Your Location's Accuracy*. As the Supreme Court determined, "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and [an]

exhaustive chronicle of location information." *Carpenter*, 138 S. Ct. at 2219. Location data from Google is similarly "exhaustive." Google routinely collects detailed location data on every user, not just when criminal activity is suspected. And when police obtain this information with a geofence warrant, it is also comprehensive, revealing every Google user who happened to pass through a given area over a given timeframe. In short, Google location data is qualitatively different from third-party business records, and regardless of the fact that Google stores it, it is entitled to a reasonable expectation of privacy.

Individuals do not voluntarily share their location information with Google, further supporting the notion that the third-party doctrine is inapposite in this context. The third-party doctrine is justified by the assumption that an individual cannot reasonably expect "information he *voluntarily* turns over to third parties" to remain private. *Smith*, 442 U.S. at 44 (emphasis added). In *Carpenter*, the Court held that cell phone users' "sharing" of their location data with their service provider is not done on a truly voluntary basis since "carrying [a cell phone] is indispensable to participation in modern society." 138 S. Ct. at 2220 (quoting *Riley*, 134 S. Ct. at 2484)). Similarly, navigation apps are exceedingly popular, with 77% of smartphone owners using them regularly, and Google Maps is far and away the most popular navigation app. Riley Panko, *The Popularity of Google Maps: Trends in Navigation Apps in 2018*, The Manifest (July 10, 2018), https://themanifest.com/app-development/popularity-google-maps-trends-navigation-apps-2018. This shows that, like owning a smartphone, using navigation software is, for many, "indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2210. Much the same could be said about Gmail or Google Search. Indeed, Google software is ubiquitous on smartphones, with Android operating systems running on 87% of devices sold in 2019. International Data Corporation, *Smartphone Market Share*, https://www.idc.com/promo/smartphone-market-

share/os, Oct. 25, 2019. Likewise, Google Maps is the most popular navigation app, used on 67% of smartphones, making it nearly six times more popular than its closest competitor Waze, which is now also owned by Google.[4] Panko, *supra*, The *Popularity of Google Maps*. And more than 90% of all internet searches use Google. Jeff Desjardins, *How Google retains more than 90% of market share*, Business Insider (Apr. 23, 2018), https://www.businessinsider.com/how-google-retains-more-than-90-of-market-share-2018-4. In short, it is not reasonable to expect ordinary phone users to avoid Google software. It cannot be that individuals must choose between their privacy and carrying a cell phone, running a Google search, or watching a YouTube video.

B. Geofence Warrants Provide the Government with Unprecedented Powers of Surveillance that Upset Traditional Expectations of Privacy.

In a series of cases addressing the power of sense-enhancing technologies "to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) (last alteration in original); *accord United States v. Jones*, 565 U.S. 400, 406 (2012). As Justice Alito explained in *Jones*, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken." 565 U.S. at 429 (Alito, J., concurring in judgment).

Technological innovations, like the ability to locate cell phones (and their users) seemingly out of thin air, remove many of these practical limitations on government surveillance capabilities. *See, e.g.*, *Prince Jones*, 168 A.3d at 714 (describing a cell-site simulator as a "powerful person-locating capability" that the government previously lacked, which is "only superficially analogous

[4] It is unclear whether use of the Waze app also contributes location data to Google's Sensorvault.

to the visual tracking of a suspect"). Recognizing the potential for technologies like these to enable invasive surveillance on a mass scale, the Court has admonished lower courts to remain vigilant "to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Carpenter*, 138 S. Ct. at 2223.

1. The data collected through a geofence warrant is extraordinarily detailed and deeply revealing.

The *Carpenter* Court noted that "like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." 138 S. Ct. at 2216. Google's Sensorvault includes GPS data, which is even more precise than the cell site location information at issue in *Carpenter*. Google, *supra*, *Find and Improve Your Location's Accuracy*. Google also locates users using "device sensors . . . or WiFi" to augment GPS's accuracy when these methods are available. Google Policies, Location Data (Nov. 20, 2018), https://policies.google.com/technologies/location-data?hl=en. As a result, Google can locate a device within approximately 20 meters, compared to "a few thousand meters" for cell site location information. Google, *supra*, *Find and Improve Your Location's Accuracy*. This level of precision can pinpoint a device to a single a building, which is significantly more detailed that the location information available from wireless carriers like AT&T or Verizon. Russell Brandom, *Police Are Filing Warrants for Android's Vast Store of Location Data*, The Verge (June 1, 2016), https://www.theverge.com/2016/6/1/11824118/google-android-location-data-police-warrants.

Indeed, Google location data can reveal information about a user's location inside constitutionally protected areas. Individuals tend to carry cell phones at all times, "into private residences, doctor's offices, political headquarters, and other potentially revealing locales," *Carpenter*, 138 S. Ct. at 2218. In this case, the 150-meter geofence fully encompasses the Journey Christian Church, which has over 3,600 followers on Facebook. Journey Christian Church,

Facebook (Oct. 25, 2019), https://www.facebook.com/JourneyRVA/. A church, like a home, is a constitutionally protected space, especially because of its obvious First Amendment significance. But when law enforcement obtained the list of Google users near the bank, it also obtained the data of Google users inside Journey Christian Church, intruding on this quintessentially protected space and violating churchgoers' reasonable expectation of privacy. Such intrusions are "presumptively unreasonable in the absence of a search warrant." *Katz,* 389 U.S. at 361; *Kyllo*, 533 U.S. at 31 ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'") (quoting *Silverman v. United States*, 365 U.S. 505 (1961)).

When Fourth Amendment searches implicate First Amendment concerns, courts should be careful to apply Fourth Amendment requirements with "the most scrupulous exactitude," *Stanford v. Texas*, 379 U.S. 476, 485 (1965). Additional safeguards may be constitutionally required to protect First Amendment freedoms, *Marcus v. Search Warrant of Property*, 367 U.S. 717, 729 (1961). But the warrant application in this case did not even mention[5] the proximity of the church or take into account the sensitive First Amendment associations and activities that the search may reveal. Instead, it unconstitutionally left "the protection of [First Amendment] freedoms to the whim of the officers charged with executing the warrant." *Stanford*, 379 U.S. at 485.

2. A Geofence Warrant Allows Law Enforcement to Retrospectively Locate Individuals in Time and Space.

In *Carpenter*, the Supreme Court distinguished cell site location information from traditional law enforcement surveillance due to "the retrospective quality of the data" which "gives police access to a category of information otherwise unknowable." *Id.* at 2218. As the Court

[5] In fact, the warrant appears to refer to the church as simply "an adjacent business." *See* Ex. A State Search Warrant at 5.

explained, it is akin to a time machine that allows law enforcement to look at a suspect's past movements, something that would be physically impossible without the aid of technology: "[i]n the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection." *Id*. Geofence warrants likewise represent an unprecedented expansion of law enforcement's ability to locate a person in time and space. They enable law enforcement to reconstruct an individual's historical movements, something that would have been impossible at the time of the adoption of the Fourth Amendment at this level of ubiquity, specificity, and cost. And as with cell cite location information, they now allow the government to "travel back in time to retrace a person's whereabouts, subject only to [Google's] retention polices." *Id.*

The Supreme Court has never blessed anything remotely like dragnet geofence warrants as a permissible means of surveillance. Like the surreptitious GPS tracking in *Jones*, 565 U.S. at 420 (Alito, J., concurring), or the acquisition of historical CSLI in *Carpenter*, 138 S. Ct. at 2217, this search could not have been conducted through visual surveillance alone. It therefore violates a reasonable expectation of privacy and is impermissible under the Fourth Amendment. *Cf. Kyllo v. United States*, 533 U.S. 27, 40 (2001) (use of a thermal imaging device is a search because the information gleaned "would previously have been unknowable without [a] physical intrusion."); *Prince Jones*, 168 A.3d 703, 714 (D.C. 2017) (use of a "cell site simulator" to locate a person through a cell phone is a search because the information is not readily available or in the public view, unlike visual surveillance or older generations of tracking devices).

C. The Acquisition of Defendant's GPS Data from Google Was a Search Under a Property-Based Approach to the Fourth Amendment.

Under a property-based theory of the Fourth Amendment, Mr. Chatrie's GPS data constitutes his "papers or effects," regardless of whether they are held by a third-party service

provider like Google. They therefore cannot be searched or seized without a *valid* warrant. *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting).

In his dissenting opinion in *Carpenter*, Justice Gorsuch opined that under a "traditional approach" to the Fourth Amendment, the protection against unreasonable searches and seizures applied as long as "a house, paper or effect was yours under law." *Id.* Justice Gorsuch drew a strong analogy between cell phone location data and mailed letters, in which people have had an established Fourth Amendment property interests for over a century, whether or not these letters are held by the post office. *Id.* at 2269. (citing *Ex parte Jackson*, 96 U.S. 727, 733 (1877)). Just as Gmail messages belong to their senders and recipients (and not to Google), so too does Google location data belong to the Google users who generate it.

Here, Mr. Chatrie's location information belongs to Mr. Chatrie. Google may be responsible for collecting and maintaining it, but even Google understands that it is the user's private data. For example, Google's privacy policy consistently refers to user data as "your information," which can be managed, exported, and even deleted from Google's servers at "your" request. Google, Privacy Policy (Oct. 26, 2019), https://policies.google.com/privacy#infodelete. These are not "business records." Businesses do not let customers export or delete the company's records at will. These are customer records—Mr. Chatrie's records. Mr. Chatrie merely entrusted his information to Google, as so many people do. He did not forfeit his Fourth Amendment interests in it.

As Justice Gorsuch explained in *Carpenter*, "[e]ntrusting your stuff to others is a bailment. A bailment is the 'delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.'" 138 S. Ct. at 2268–69 (Gorsuch, J., dissenting). Here, Google is the bailee, and it owes a duty to the bailor, Mr. Chatrie, to keep his data safe. This

arrangement is apparent from Google's privacy policy. Google is not allowed to do whatever it wishes with Mr. Chatrie's data. While Google reserves the right to use it for advertising or development purposes, it also promises not to disclose it to "companies, organizations, or individuals outside of Google," subject to a short list of explicit exceptions.[6] In other words, Mr. Chatrie retains the right to exclude others from his location data, a quintessential feature of property ownership. *See* William Blackstone, 2 Commentaries on the Laws of England *2 (1771) (defining property as "that sole and despotic dominion … exercise[d] over the external things … in total exclusion of the right of any other."); *Loretto v. Teleprompter Manhattan CATV Corp*., 458 U.S. 419, 435 (1982) (calling the right to exclude "one of the most treasured strands" of the property rights bundle); *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979) (calling the right to exclude "one of the most essential sticks" in the property rights bundle).

Law enforcement eviscerated Mr. Chatrie's right to exclude others from his location data, which Google held in trust for him. This trespass constitutes a Fourth Amendment search and seizure, no less than a violation of one's "reasonable expectation of privacy."

II. A Geofence Warrant Is an Unconstitutional General Warrant.

A geofence warrant, like the warrant in this case, is a general warrant, repugnant to the Constitution. It is the epitome of the "dragnet" law enforcement practice that the Supreme Court feared in *Knotts*, 460 U.S. at 284, sweeping up the location data of untold innocent individuals in the hopes of finding one potential lead. It is inherently overbroad and lacking particularity by design. It cannot satisfy the Fourth Amendment with "scrupulous exactitude" because it is

[6] Google, Privacy Policy (Oct. 26, 2019), https://policies.google.com/privacy#infosharing. One of these exceptions is "For legal reasons," but this is not a free pass to hand over user data to law enforcement. It is implied that legal process must be valid, which includes establishing probable cause and following the strictures of the Fourth Amendment, not just submitting the proper form. *See* Jim Harper, *The Fourth Amendment and Data: Put Privacy Policies in the Trial Record*, The Champion, Jul. 2019, at 21.

inherently antithetical to the Fourth Amendment. The Court should find that geofence warrants like this one are categorically invalid and void *ab initio.*

A. The Fourth Amendment Forbids General Warrants.

As the Supreme Court has repeatedly recognized, opposition to general warrants "helped spark the Revolution itself," demonstrating the degree to which they offend the most basic principles of American liberty. *Carpenter*, 138 S. Ct. at 2213; *see also Riley*, 573 U.S. at 403; *Stanford*, 379 U.S. at 481; *Marcus*, 367 U.S. at 728. The Virginia Declaration of Rights, like other founding documents, also reflects this colonial hostility to general warrants by explicitly and categorically prohibiting them:

> That general warrants, whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, *or to seize any person or persons not named*, or whose offense is not particularly described and supported by evidence, are grievous and oppressive, and ought not to be granted.

Va. Const. art. I, § 10 (emphasis added); *see also Zimmerman v. Town of Bedford*, 134 Va. 787, 800 (1922). They are likewise forbidden by Virginia Code § 19.2–54 ("no general warrant for the search of a house, place, compartment, vehicle or baggage shall be issued"); *see also Morke v. Commonwealth*, 14 Va. App. 496, 500 (1992) (stating general warrants are proscribed by both the Fourth Amendment and Code § 19.2–54).

At the time of the Revolution, a general warrant meant a warrant that failed to identify the people to be arrested or the homes to be searched. *See Steagald v. United States*, 451 U.S. 204, 220 (1981) ("The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched."). For example, one of the specific cases that gave rise to the Fourth Amendment was *Wilkes v. Wood*, 98 Eng. Rep. 489, 490 (1763), which concerned a general warrant that ordered

the king's messengers to "apprehend and seize the printers and publishers" of an anonymous satirical pamphlet, the *North Briton* No. 45. The warrant did not specify which houses to search or whom to arrest, but officials ransacked five homes, broke down 20 doors, rummaged through thousands of books and manuscripts, and arrested 49 people. *See* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 Ind. L.J. 979, 1007 (2011). The *Wilkes* court condemned the warrant because of the "discretionary power" it gave officials to decide where to search and what to take. 98 Eng. Rep. at 498. The case became wildly famous in the American colonies, one of three influential English cases that led to the rejection of general warrants.[7]

One reason the Founders opposed general warrants was because of the discretion they gave to officials. They placed "'the liberty of every man in the hands of every petty officer'" and were therefore denounced as "'the worst instrument of arbitrary power." *Stanford*, 379 U.S. at 481 (quoting James Otis). The other reason was that general warrants allowed the government to target people without any evidence of criminal activity, turning the concept of innocent until proven guilty on its head. Donohue, 83 U. Chi. L. Rev. at 1317. Instead of having information that the person or place to be searched is engaged in illegal activity, general warrants presume guilt, establishing innocence only after a search. *Id.* Prohibiting such "promiscuous" searches therefore served to protect not only individual rights, but also a cornerstone of American liberty. *Id.*

Thus, for example, no valid search warrant would permit the police to search every house in a neighborhood or pat down everyone in sight. *See United States v. Glenn*, 2009 WL 2390353, at *5 (S.D. Ga. 2009) ("The officers' 'generalized' belief that some of the patrons whom they had

[7]*See generally*, Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1196 (2016). In addition to *Wilkes v. Wood*, the cases were *Entick v Carrington*, 19 How St Tr 1029 (CP 1765), and *Leach v Money*, 19 How St Tr 1001 (KB 1765).

targeted for a systematic patdown might possibly have a weapon was insufficient to justify a 'cursory' frisk of everyone present."); *Commonwealth v. Brown*, 68 Mass. App. Ct. 261, 262 (Mass. App. Ct. 2007) (holding that a warrant "authorizing a search of 'any person present' . . . resulted in an unlawful general search."); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding that a "warrant to search all suspected places [for stolen goods]" was unlawful because "every citizen of the United States within the jurisdiction of the justice to try for theft, was liable to be arrested"). Yet, with a geofence warrant, law enforcement can do just that, searching inside every home, vehicle, purse, and pocket in a given area, without particularized suspicion to search any of them.

B. A Geofence Warrant Is A General Warrant.

A geofence warrant, like the one in this case, is a modern-day incarnation of the historically reviled general warrant. It is the digital equivalent of searching every home in the neighborhood of a reported burglary, or searching the bags of every person walking along Broadway because of a theft in Times Square. Without the name or number of a single suspect, and without ever demonstrating any likelihood that Google even has data connected to a crime, law enforcement invades the privacy of tens or hundreds or thousands of individuals, just because they were in the area. *Cf. Sibron v. New York*, 392 U.S. 40, 63–64 (1968) (holding that "[t]he suspect's mere act of talking with a number of known narcotics addicts over an eight-hour period" did not give rise to either reasonable suspicion or probable cause to search him).

The Supreme Court has always been "careful to distinguish between [] rudimentary tracking . . . and more sweeping modes of surveillance," in deciding whether a search is constitutional. *Carpenter*, 138 S. Ct. at 2215 (citing *Knotts*, 460 U.S. at 284). Geofence warrants fall on the "sweeping" end of this spectrum, as they potentially affect everyone. They represent

the kind of surveillance that the Supreme Court cautioned against in *Knotts*, noting that "if such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." 460 U.S. at 283–84. That time is now.

A comparison to the "rudimentary tracking" in beeper cases such as *Knotts* and *Karo* illuminates the drastically different, indiscriminate-dragnet nature of a geofence warrant. In the beeper cases, the government only sought to track *one* individual. To do so, law enforcement first needed to identify the individual, and then to physically install a tracking device on an object that was in their possession. With a geofence warrant, however, the government no longer needs identify a suspect. Instead, "[w]ith just the click of a button, the government can access [Google's] deep repository of historical location information at practically no expense." *Carpenter*, 138 S. Ct. at 2218; *see also United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) ("Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive"). Because of the ubiquity of Google software on cell phones, Sensorvault includes location data on many of the 400 million devices in the United States—"not just those belonging to persons who might happen to come under investigation," meaning that "this newfound tracking capacity runs against everyone" who uses Google. *Carpenter*, 138 S. Ct. at 2218.

Geofence warrants pose the same type of threat as colonial-era general warrants "which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 134 S. Ct. at 2494. As in this case, they are the product of unrestrained searches of constitutionally protected spaces, like the Journey Christian Church. And they result

in rummaging through the digital papers and effects of large numbers of unknown, unnamed people, all or almost all of whom are admittedly innocent.

C. A Geofence Warrant Cannot Satisfy the Probable Cause or Particularity Requirements.

By design, a geofence warrant does not specify the individuals or individual Google accounts to be searched. Rather, the purpose is to search across millions of unknown user accounts and then identify specific accounts that law enforcement would like to search further. As a result, however, geofence warrants are inherently incapable of meeting the probable cause and particularity requirements of the Fourth Amendment, and are therefore general warrants.

Geofence warrants are intentionally overbroad. In contrast to warrants authorizing the acquisition of location data about a single individual suspected of a criminal offense, geofence warrants identify all Google users merely due to their proximity to a crime scene. But as the Supreme Court has held on more than one occasion, "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) (citing *Sibron*, 392 U.S. at 62–63); *see also United States v. Di Re*, 332 U.S. 581, 587 (1948) (holding that a person, by mere presence in a suspected car, does not lose immunities from search of his person to which he would otherwise be entitled). Consequently, there is an abject absence of individualized suspicion for any, let alone all, of the individuals whose Google data were searched by the warrant. Of course, it would have been difficult to establish probable cause for the location information of every Google user near the bank, as the government acknowledges that most of the data belongs to innocent people. But the convenience of gathering location information on all of those individuals with a single warrant to Google does not obviate the requirements of the Fourth Amendment. *Riley*, 134 S. Ct. at 2493 (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)); *Carroll v.*

United States, 267 U.S. 132, 153–54 (1925) ("It would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor, and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search."). The warrant is void for lack of probable cause.

Similarly, a geofence warrant is not remotely particularized. The purpose of the particularity requirement is to prevent general warrants, which it does by "limiting the authorization to search the specific areas and things for which there is probable cause to search." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). With respect to seizures, the Fourth Amendment demands that "nothing is left to the discretion of the officer executing the warrant." And where, as here, there are significant First Amendment concerns—especially due to the proximity of a church—the particularity requirement takes on heightened importance. *Stanford*, 379 U.S. at 485; *Marcus*, 367 U.S. at 729; *A Quantity of Copies of Books v. Kansas*, 378 U.S. 205, 212 (1964).

A geofence warrants leaves the question of whose data to search and seize almost entirely the discretion of the executing officers. It does not "particularly describe the 'things to be seized,' let alone identify the name of a single suspect Google user, phone number, or account. *Dalia v. United States*, 441 U.S. 238, 255 (1979) (citing *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Instead, it identifies Google headquarters as the place to be searched and requests location data from *all* Google users near a given location. Although the data is "anonymized" initially, it does not stay that way. Rather, the warrant leaves it up to the police to "narrow down the list" by some unknown or unstated method before the officers decide which accounts to deanonymize and search further. *See* Ex. A State Search Warrant at 2. Law enforcement engage in multiple rounds of back-and-forth with Google—not the independent magistrate envisioned by the Fourth Amendment—

to decide whose data they would review. Paired with the sweeping scope and absence of probable cause, the lack of particularity in geofence warrants make them unconstitutional general warrants.

D. This Geofence Warrant is Overbroad and Lacking Particularity

Even if geofence warrants are not categorically impermissible, the geofence warrant obtained in this case is unconstitutionally overbroad and lacks particularity.

First, Virginia police did not have probable cause to believe that the bank was robbed by a Google user. While the warrant application does state that the robber could be seen using a cell phone, there is no evidence to show that it was an Android phone or that he or she used a Google service within the initial one-hour window identified in the warrant. The application cites the general popularity of cell phones, but does not provide any facts to suggest that Google specifically would have data pertaining to the perpetrator of this crime. It did not allege that bank robbers frequently use Google or state that a teller had noticed the phone's make and model. If the robber had an iPhone and did not use Google services between 4:20 and 5:20 p.m., then Google would not have a record of the phone's location during that time.[8]

Second, the warrant does not specify which Google accounts it seeks to search, presumably due to the lack of probable cause to search any specific Google user. Even the 150-meter radius is not sufficiently particular. Rather than a requesting data for just the bank and parking lot, the warrant included the entirety of the church next door. Furthermore, a three-step, back-and-forth process with the recipient of a warrant is not a substitute for particularizing that warrant at the outset. Instead, it is an unconstitutional delegation of discretion to the executing officers. The

[8] Likely for this reason, the use of geofence warrants elsewhere has frequently failed to identify suspects. *See* Tyler Dukes, *To find suspects, police quietly turn to Google*, WLAR (Mar. 15, 2018), https://www.wral.com/Raleigh-police-search-google-location-history/17377435/ (finding that "only one person has been arrested for any of the crimes in which police approached Google for data on *thousands of users*" across the four investigations).

issuing court had no information on how many people were likely to be initially affected. And it had no role in deciding which of those people would be subject to further search, outside the geofence, wherever they happened to be. Indeed, the warrant permits police to obtain location data from *anywhere outside* the geofence for an unknown subset of users, identified solely by investigators, with no additional showing or judicial involvement. *See* Ex. A State Search Warrant at 2. Finally, the court had no role in deciding which or how many people would have their data deanonymized and searched further still. The warrant left everything up to the discretion of the executing officers, violating the Fourth Amendment's particularity requirement.

III. The Good Faith Exception Does Not Apply

Under the good-faith exception to the exclusionary rule, evidence derived from an unconstitutional search should not be suppressed when it is obtained in reliance on a facially valid warrant. *United States v. Leon*, 468 U.S. 897 (1984). The Supreme Court has emphasized, however, that "in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *Id.* at 922-23. There, the good faith exception would not apply, and suppression would be appropriate "if the officers . . . could not have harbored an objectively reasonable belief in the existence of probable cause." *Id.* at 926. Suppression is also appropriate where "a warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be searched—that the executing officers cannot reasonably presume it to be valid." *Id.*

Here, a reasonable law enforcement officer could not have presumed that such an overbroad, unparticularized warrant would be valid. The police knew they did not have a suspect, let alone probable cause to search any specific person or place. Instead, they sought every Google user's location data near a bank at rush hour—with no evidence that the robber had ever used

Google. They then exercised complete discretion in deciding which accounts to search further, deanonymize, and obtain additional information about. The deficiencies of this geofence warrant—its absence of probable cause and particularity—are readily apparent, casting it within the circumstances described in *Leon* and making the good faith exception to the exclusionary rule inapplicable.

CONCLUSION

This is a case of first impression, but the Court should treat the geofence warrant here as any other general warrant: repugnant to the Constitution. Geofence warrants represent an unprecedented expansion of the government's surveillance capabilities. *Carpenter*'s emphasis on the degree to which location data obtained by law enforcement is sensitive or "deeply revealing" shows that courts are recognizing the need to treat cell phone data differently from physical records. Based on the sensitivity of these records and the scope of the search, geofence warrants are Fourth Amendment searches of the unreasonable variety. The warrant obtained in this case implicates First Amendment concerns, and as such must withstand "scrupulous exactitude" under the Fourth Amendment. Yet this geofence warrant cannot even survive the probable cause and particularity under the Fourth Amendment. Instead, the warrant functions as a general warrant, thus not meeting the higher First Amendment standard. Finally, because the good faith exception cannot apply to a warrant no reasonable law enforcement officer would in good faith rely on, this geofence warrant is an unconstitutional search, and we therefor request that its fruits be suppressed.

Respectfully submitted,

OKELLO T. CHATRIE

By: /s/
Michael W. Price
NY Bar No. 4771697 (pro hac vice)
Counsel for Defendant

National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

/s/
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on October 29, 2019, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

/s/
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION FOR SUPPRESSION OF EVIDENCE OBTAINED PURSUANT TO GOOGLE GEOFENCE WARRANT

The United States of America, by its undersigned attorneys, moves this Court to deny Defendant Okello T. Chatrie's motion to suppress evidence obtained from Google, LLC ("Google") pursuant to a search warrant for GeoFence location information (the "GeoFence warrant"). (ECF No. 29.)

The warrant authorized disclosure from Google of two hours of location information associated with electronic devices that were, within a one-hour interval, within 150 meters of the site of a bank robbery. This Court should deny the defendant's motion for three reasons. First, investigators did not conduct a search under the Fourth Amendment when they obtained this information from Google. Second, the GeoFence warrant complied with the Fourth Amendment, as it was issued based on probable cause and specified its object with particularity. Third, suppression is inappropriate because investigators relied on the warrant in good faith.

I. BACKGROUND

At approximately 4:50 p.m. eastern standard standard time, on May 20, 2019, a then-unknown male entered the Call Federal Credit Union in Midlothian, Virginia with a firearm. While the man stood in line, victim-teller J.B. asked another teller, J.W., to assist this customer

when he reached the counter. When he reached J.W.'s station, the man presented a handwritten note. That note read, in part, "I got your family as hostage and I know where you live, If you or your coworker alert the cops or anyone your family and you are going to be hurt . . . I need at least 100k." After J.W. told him that she did not have access to that amount of money, the armed robber pulled out a silver and black handgun. Waving the firearm around, he then directed J.W., other Call Federal Credit Union employees, and customers to move to the center of the lobby and get on the floor. Once there, the armed robber led victims behind the teller counter and into a back room where the Credit Union's safe was located.

Once in the back room, he ordered everyone to their knees at gunpoint and demanded that the bank manager open the safe. The Credit Union manager, fearing for his life, obliged by opening the safe and handing over $195,000 in United States currency.

After the armed robbery, victims dialed 911 to request assistance. When law enforcement arrived, they reviewed surveillance video from the credit union and determined that the armed robber entered the credit union from an area behind a nearby church, held a cellular telephone to his ear when entering the credit union, and ran back towards the church after the robbery. An employee of that church explained to law enforcement that he saw a suspicious individual in a newer model, blue Buick sedan prior to the time of the robbery.

Investigators knew that Google stored location information that could help them apprehend and convict the robber. Google obtains and stores its customers' location information for a wide variety of purposes. Google explains: "From driving directions, to making sure your search results include things near you, to showing you when a restaurant is typically busy, location can make your experiences across Google more relevant and helpful. Location information also helps with some core product functionality, like providing a website in the right language or helping to

keep Google's services secure." How Google Uses Location Information (available at https://policies.google.com/technologies/location-data).

In particular, Federal Bureau of Investigation Task Force Officer Josh Hylton knew that in response to a "GeoFence" warrant, Google could produce location and identity information from accounts associated with electronic devices present in a specified area at a specified time. In one of his previous robbery investigations, an Assistant United States Attorney had reviewed his application for a federal GeoFence search warrant, and he subsequently applied for and obtained a GeoFence warrant in that investigation from a United States Magistrate Judge. In addition, he had previously discussed GeoFence warrants with a Virginia state prosecutor, who had expressed no concerns about their constitutionality.

On June 14, 2019, Task Force Officer Hylton sought and obtained a GeoFence warrant from the Chesterfield Circuit Court of Virginia. His statement of probable cause began by describing the facts of the robbery, including that prior to the robbery, the robber held a cell phone and appeared to be speaking with someone. *See* State GeoFence Warrant at 4.[1] The statement then explained why there was reason to believe that Google would have evidence pertaining to the robbery. Among other facts, the statement disclosed: (1) that as of 2013, 56% of cell phones were smartphones; (2) that "[n]early every" Android phone "has an associated Google account"; (3) that Google "collects and retains location data" from such devices when the account owner enables Google location services; and (4) that Google collects location information from non-Android smartphones if the devices are "registered to a Google account and the user has location services enabled." *Id.* at 5. Magistrate David Bishop issued the GeoFence warrant upon a finding of

[1] The United States will provide a copy of the entire GeoFence search warrant application to the Court in conjunction with this motion.

probable cause. *Id.*

The GeoFence warrant specified a target geographical area, identified as a circle of radius 150 meters around a specific latitude and longitude point near the bank. *See id.* at 3. It authorized disclosure of location information over a two-hour interval (from 3:50 pm to 5:50 pm) from accounts associated with devices within this target area at some point during a one-hour interval that included the robbery (from 4:20 pm to 5:20 pm). *See id.* at 2-3. The warrant also authorized disclosure of specified customer identity information associated with these accounts, including user name and email address. *See id.* at 3.

The warrant authorized this disclosure through a three-step process that enabled law enforcement to "narrow down" the information disclosed by Google and thus obtain less than the maximum amount of information covered by the warrant. *Id.* at 2-3. The warrant directed that in the first step, Google was to disclose location information for devices present in the target area during the hour of the robbery, but not the identity information associated with the devices. *See id.* at 2. In the second step, law enforcement was to review the anonymized location information produced by Google and identify the accounts of interest, and Google was then to disclose location information for those accounts over the full two-hour interval, both within and outside of the target area, but again without disclosing identity information. *See id.* at 2-3. In the third step, law enforcement was to identify accounts that remained of interest, and Google was to disclose subscriber identity information for those accounts. *See id.* at 3.

Investigators followed this three-step process when they executed the warrant. In step one, Google produced one hour of location information within the target area for 19 anonymized accounts. In step two, investigators identified nine of those accounts for further disclosure, and Google produced two hours of anonymized location information for those nine accounts. The

anonymized information showed one account of particular interest (hereinafter, the "Chatrie Account"), as it was associated with a device that: (1) was near the church prior to the robbery at the same time that the church witness recalled seeing the suspicious individual; (2) inside the credit union during the robbery; and (3) immediately left the area following the robbery via the area near the church. In step three, law enforcement requested and obtained subscriber information for three accounts, including the Chatrie Account, which belonged to the defendant. This information included the defendant's email address and that he used an Android phone and Google Location History.

As the owner of an Android phone, the defendant had affirmatively opted-in to Google's use and storage of his location information. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122) ("You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.").[2] He also had the ability to delete his location history. *See id.* In addition, he agreed to disclose his location information to Google for multiple purposes, including for Google to provide "personalized" services to him (including "content and ads" or "driving directions") and for Google to develop new services. *See id.*

Subsequent investigation provided further evidence that the defendant was the robber. On September 17, 2019, the grand jury returned a two-count Indictment for Forced Accompaniment during an Armed Credit Union Robbery, in violation of 18 U.S.C. § 2113(e), and Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A)(i).

[2] Google archives changes over time to its Privacy Policy. *See* https://policies.google.com/privacy/archive. Here, the United States references the Privacy Policy that was in effect from January 22 to October 14, 2019, a period which includes the bank robbery.

The defendant pleaded not guilty on October 1, 2019, and trial was scheduled for December 3, 2019, through December 5, 2019, at 9:00 a.m. before the Honorable M. Hannah Lauck.

On October 29, 2019, the defendant filed the Motion to Suppress that is subject of this response.

II. ARGUMENT

A. The Defendant Had No Reasonable Expectation of Privacy in Two Hours of Google Location Information

As set forth below, the defendant had no reasonable expectation of privacy in any of the information disclosed by Google pursuant to the GeoFence warrant. The defendant argues that he had a reasonable expectation of privacy in his location information under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), but *Carpenter* held only that the government infringes a cell phone owner's reasonable expectation of privacy when it accesses seven days or more of cell phone location information. *See Carpenter*, 138 S. Ct. at 2217 n.3. Here, the United States' acquisition of two hours of the defendant's location information is governed by the long-standing principle that a person has no reasonable expectation of privacy in information disclosed to a third party and then conveyed by the third party to the government.[3]

1. Obtaining Two Hours of the Defendant's Location Information Was Not a Search Under *Carpenter*

The defendant claims based on *Carpenter* that he had a reasonable expectation of privacy in the two hours of location information disclosed by Google, but *Carpenter* does not bear the weight he places on it. In *Carpenter*, the Supreme Court determined that individuals have a

[3] Google also disclosed to the government the defendant's basic subscriber information, including email address, Google Account ID, and Google services used. In *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010), the Fourth Circuit held that a subscriber has no reasonable expectation of privacy in such information. The defendant does not claim any protected privacy interest in this information.

"reasonable expectation of privacy in the whole of their physical movements," and it held "that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search." *Carpenter*, 138 S. Ct. at 2217 & n.3.

The Court emphasized that its decision was "a narrow one." *Carpenter*, 138 S. Ct. at 2220. It explicitly declined to determine whether there is a "limited period" for which the government can acquire cell phone location information without implicating the Fourth Amendment. *Id.* at 2217 n.3. It also explicitly refused to decide whether obtaining a cell tower dump constituted a Fourth Amendment search. *See id.* at 2220. This limitation is relevant here because tower dump information is similar to the information disclosed pursuant to the GeoFence warrant. A tower dump includes "information on all the devices that connected to a particular cell site during a particular interval." *Id.* Here, the GeoFence warrant sought information on all devices that were within a particular area during a particular interval.

Although *Carpenter* declined to resolve whether obtaining two hours of cell phone location information constitutes a search, *Carpenter*'s reasoning suggests it does not, because *Carpenter* is focused on protecting a privacy interest in long-term, comprehensive location information. The Court began its opinion by framing the question before it as "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Carpenter*, 138 S. Ct. at 2212. The Court emphasized that long-term cell-site information created a "comprehensive record of the person's movements" that was "detailed" and "encyclopedic." *Id.* at 2216–17. It explained that "this case is not about 'using a phone' or a person's movement at a particular time. Rather, the Court explained, the case concerned a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* at 2220. By this standard, the government did not

conduct a search when it obtained the defendant's location information pursuant to the GeoFence warrant.

Two hours of location data is only 1/84th of the period that *Carpenter* held constituted a search, and it does not provide the sort of "all-encompassing record of the holder's whereabouts" and "intimate window into a person's life" that concerned the Court. *Carpenter*, 138 S. Ct. at 2217. Rather than providing an encyclopedic chronicle of the defendant's life, the information disclosed by Google provided a summary of his location for less than half an afternoon. This information is not quantitatively or qualitatively different from information that could be obtained from other sources, such as surveillance video or live witnesses.

The United States is not aware of any judicial opinions addressing whether a GeoFence warrant infringes a reasonable expectation of privacy under *Carpenter*. The Seventh Circuit, however, held that *Carpenter* "does not help" a robber identified via tower dumps. *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019). The court explained that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near one location (the victim stores) at one time (during the robberies))." *Id.* at 611.

The defendant's additional *Carpenter*-related arguments do not establish that the government infringed his reasonable expectation of privacy. He argues that Google's information about its users' location is "more precise than the cell site location information at issue in *Carpenter*," ECF No. 29 at 12, but the Supreme Court in *Carpenter* stated that cell-site information "is rapidly approaching GPS-level precision," and *Carpenter*'s holding "t[ook] account of more sophisticated systems that are already in use or in development." *Carpenter*, 138 S. Ct. at 2218-19. Thus, because the Supreme Court grounded *Carpenter*'s holding in an assumption that cell-site information would approach the precision of GPS, any distinction in precision between them

cannot create enhanced Fourth Amendment protections for GPS information.

The defendant also argues that GeoFence information "Allows Law Enforcement to Retrospectively Locate Individuals in Time and Space," ECF No. 29 at 13, but that fact does not distinguish GeoFence information from a wide variety of other business records, or even from witness testimony. For example, credit card records, landline telephone records, employee time sheets, and IP address records may enable law enforcement to retrospectively locate individuals at particular points in time. However, like the GeoFence information, none of these records provide a comprehensive inventory of the whole of a person's movements, and the government does not infringe the privacy interest protected by *Carpenter* when it obtains them. *See, e.g.*, *United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. June 13, 2019) (unpublished) (holding that defendant had no reasonable expectation of privacy in IP address information, even after *Carpenter*).

2. The Defendant Has No Reasonable Expectation of Privacy in Location Information He Disclosed to Google

Because *Carpenter* does not create a reasonable expectation of privacy in two hours of location information, Google's disclosure of that information to the United States is subject to the long-standing principle that an individual retains no reasonable expectation of privacy in information revealed to a third party and then disclosed by the third party to the United States. For decades, the Supreme Court has repeatedly invoked this third-party doctrine in cases ranging from private communications to business records, and this principle applies here to the defendant's location information.

For example, in *Hoffa v. United States*, 385 U.S. 293 (1966), the Court applied the third-party doctrine to incriminating statements made in the presence of an informant. The Court held that the Fourth Amendment did not protect "a wrongdoer's misplaced belief that a person to whom

he voluntarily confides his wrongdoing will not reveal it." *Id.* at 302. A decade later the Supreme Court rejected a Fourth Amendment challenge to a subpoena for bank records in *United States v. Miller*, 425 U.S. 435 (1976). The Court held "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443. *See also SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (applying the third-party doctrine to financial records in the hands of a third-party).

The Supreme Court also relied on this principle in *Smith v. Maryland*, 442 U.S. 735 (1979), when it held that a telephone user had no reasonable expectation of privacy in dialed telephone number information. First, the Court stated that "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. In addition, the Supreme Court further held that even if the defendant had a subjective expectation of privacy in his dialed telephone numbers, "this expectation is not one that society is prepared to recognize as reasonable." *Id.* at 743 (internal quotation marks omitted). The Court explained that the user "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." *Id.* at 743-44.

The defendant therefore had no reasonable expectation of privacy in Google's records of his location because he voluntarily conveyed his location to Google in exchange for receiving the benefits of Google services. Because Google location service is an opt-in service, the defendant had previously taken an affirmative step to disclose his location information to Google. Moreover,

he agreed that Google would have access to his location information for purposes ranging from providing him with targeted advertising or assistance with driving directions to Google's development of new services. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122). These facts demonstrate that the defendant voluntarily disclosed his location information to Google, and the United States did not infringe his reasonable expectation of privacy when it obtained from Google information about his device's location during a two-hour interval.

Finally, the fact that the defendant voluntarily disclosed his location information to Google is confirmed by the reasoning of *Carpenter*. *Carpenter* concluded that cell-site information was not voluntarily disclosed to the phone company for two reasons, neither applicable here. First, the Court held that carrying a cell phone "is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. In contrast, although Google services are frequently helpful and convenient, most may be used without turning on Google location services, and using Google services with location enabled is not essential to participation in modern society. Google location services are no more indispensable than having a bank account or making a phone call, and bank records and dialed telephone number information remain unprotected by the Fourth Amendment under *Miller* and *Smith*. Second, *Carpenter* held that cell-site information is collected "without any affirmative act on the part of the user beyond powering up" and that "there is no way to avoid leaving behind a trail of location data." *Id.* In contrast, in order for Google to have his location information, the defendant had to affirmatively opt in, and he also retained the ability to delete his information. Finally, a cell phone user's disclosure of location information to the phone company is merely incidental to receiving communication service from the company, but a device owner's disclosure of location information to Google is the central prerequisite to obtaining Google

location services. The defendant thus voluntarily disclosed his location information to Google, and Google's disclosure of that information to the government did not infringe upon his reasonable expectation of privacy.

The defendant also asserts that the GeoFence warrant intruded on the reasonable expectation of privacy of others, ECF No. 29 at 13, but this argument fails for two separate reasons. First, the Supreme Court has squarely held that Fourth Amendment rights "may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). The defendant therefore lacks standing to challenge the government's acquisition of others' location information. *See, e.g.*, *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (rejecting defendant's argument that investigator's use of a cell-site simulator violated the privacy rights of third parties, because the defendant was "not entitled to invoke the rights of anyone else; suppression is proper only if the defendant's own rights have been violated"). Second, these other individuals also voluntarily disclosed their location information to Google. Google's disclosure of their location information therefore did not infringe their Fourth Amendment rights either.

Finally, the defendant claims that obtaining his information from Google constitutes a search under "a property-based theory of the Fourth Amendment." ECF No. 29 at 14. This argument is rooted in Justice Gorsuch's solo dissent in *Carpenter*, where he discussed a transformation of the Fourth Amendment that would jettison not only *Smith* and *Miller*, but also the reasonable expectation of privacy test of *Katz v. United States*, 389 U.S. 347 (1967). *See Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J., dissenting). Ultimately, Justice Gorsuch concluded that *Carpenter* forfeited this new argument because he did not raise it below. *See id.* at 2272. Regardless, a solo dissent is not the law, and *Smith*, *Miller*, and *Katz* remain binding on this Court.

Under existing law, Google's disclosure of location information to the government did not infringe upon any reasonable expectation of privacy.

B. The GeoFence Warrant Satisfied the Fourth Amendment

The GeoFence warrant did not remotely resemble a general warrant. A general warrant "specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). In contrast, the GeoFence warrant authorized the government to obtain from Google limited and specified information directly tied to a particular robbery at a particular place and time. As set forth below, because the warrant was supported by probable cause and specified its object with particularity, the defendant's argument that the warrant was a general warrant is without merit. *See* ECF No. 29 at 16-24.

More broadly, the facts of this case illustrate why a warrant that requires disclosure of information about devices in a particular place at a particular time is neither a general warrant nor, as the defendant asserts, "repugnant to the Constitution." ECF No. 29 at 16. When law enforcement officers sought the warrant, they were investigating a serious violent crime, and they had reason to believe that the perpetrator was reasonably likely to commit other similar offenses if not identified and apprehended. The GeoFence warrant allowed them to solve the crime and protect the public by examining a remarkably limited and focused set of records from Google: location information over a two-hour interval of three identified and six unidentified individuals, and limited location information over a one-hour interval of ten other unidentified individuals. Rather than being "repugnant to the Constitution," this investigative technique involved no unreasonable search or seizure and should be encouraged, not condemned.

1. The Geofence Affidavit Established Probable Cause

Probable cause requires only "a fair probability, and not a prima facie showing, that contraband or evidence of a crime will be found in a particular place." *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (internal quotation marks omitted)). It is "not a high bar." *Id.* (quoting *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018). In addition, this Court does not conduct *de novo* review concerning the existence of probable cause: "the duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004) (quoting *Gates*, 462 U.S. at 238–39).

Here, the affidavit in support of the warrant established an ample basis for the issuing magistrate's finding of probable cause. First, it established that an unknown subject committed an armed bank robbery at a particular place and time. *See* State GeoFence Warrant at 4. Second, it established that at the bank prior to the robbery, the robber held the cell phone to his ear and appeared to be speaking with someone. *See id.* Third, the affidavit established that even as of 2013, the majority of cell phones were smartphones. *See id.* at 5. Fourth, it established a connection between smartphones and Google location information. It explained that "[n]early every" Android phone "has an associated Google account," and that Google "collects and retains location data" from such devices when the account owner enables Google location services. *Id.* It also explained that Google can collect location information from non-Android smartphones if the devices are "registered to a Google account and the user has location services enabled." *Id.* From this information, there was a substantial basis for the magistrate to find probable cause to believe that Google possessed evidence related to the robbery.

The defendant objects that there was no probable cause to believe that the bank was robbed by a Google user, *see* ECF No. 29 at 23, but his argument ignores that the probable cause standard requires only a fair probability that evidence will be found at the place searched. The defendant posits a situation in which Google would not have had the robber's location information—"[i]f the robber had an iPhone and did not use Google services"—but he does not dispute that it was likely that Google would have information regarding Android users or that it would have information regarding some non-Android users. ECF No. 29 at 23. The magistrate therefore had a substantial basis for his finding of probable cause.

The United States is unaware of any decisions addressing Fourth Amendment challenges to GeoFence warrants, but one district court recently rejected a similar challenge to cell tower dump warrants. In *United States v. James*, No. 18-cr-216, 2019 WL 325231 (D. Minn. Jan. 25, 2019), the government used tower dump warrants to solve a series of robberies. The defendant there argued that there was no probable cause for the warrants because it was "unknown whether a phone was used by the suspect before or after the robbery." *Id.* at *3. Nevertheless, the district court found that probable cause existed based on the affiant's representations about the "ubiquitous nature" of cell phones, the likelihood of criminals using cell phones, and the storage by cell phone companies of location information. *Id.* Here, where the robber used his phone just before the robbery, the basis for the magistrate's finding of probable cause was at least as strong as in *James*.

Furthermore, the probable cause established by the affidavit supported obtaining Google information for evidentiary purposes other than identifying the robber directly. As the affidavit explained, location information from Google could also "identify potential witnesses" and "assist investigators in forming a fuller geospatial understanding and timeline" of the robbery. State GeoFence Warrant at 5. The warrant appropriately sought such information, as a search warrant

may be issued to obtain evidence to "aid in a particular apprehension or conviction." *Warden v. Hayden*, 387 U.S. 294, 307 (1967).

Messerschmidt v. Millender, 565 U.S. 535 (2012), demonstrates that the Supreme Court does not narrowly construe what may constitute evidence for purposes of a search warrant. In *Messerschmidt*, police obtained a warrant for "all guns and gang-related material" in connection with a known gang member shooting at his ex-girlfriend. *Id.* at 539. In a civil suit under 42 U.S.C. § 1983, Millender challenged the warrant as overbroad, but the Supreme Court rejected the suit based on qualified immunity. *See id.* The Court provided multiple reasons why it was not unreasonable for a warrant to seek "all gang-related materials" in connection with someone shooting at his ex-girlfriend. These reasons included that it could "help to establish motive," that it could be "helpful in impeaching [the shooter]," that it could be helpful in "rebutting various defenses," and that it could "demonstrat[e] [the shooter's] connection to other evidence." *Id.* at 551-52.

Similarly, the issuing magistrate here had multiple reasons to believe that the location information for those present at the robbery would constitute evidence. Investigators could use the location information directly to reconstruct what took place at the crime scene at the time of the crime. They could use it to identify the robber and any accomplices. They could use it to identify potential witnesses and obtain further evidence. They could use it to corroborate and explain other evidence, including surveillance video. They could use it to rebut potential defenses raised by the robber, including an attempt by the robber to blame someone else for his crime. Thus, although the defendant is correct that proximity to criminals does not alone give rise to probable cause that he committed a crime, *see* ECF No. 29 at 21, here probable cause existed for the location information sought by the warrant. The issuing magistrate had a substantial basis for finding

probable cause to believe that Google possessed location information regarding the scene of the robbery, and this Court should therefore deny the defendant's motion to suppress.

Finally, the defendant repeatedly emphasizes that the GeoFence warrant collected information about persons not suspected of criminal activity, but this fact does not aid his Fourth Amendment argument. The Supreme Court has held that "it is untenable to conclude that property may not be searched unless its occupant is reasonably suspected of crime." *Zurcher v. Stanford Daily*, 436 U.S. 547, 559 (1978). Instead, a search warrant "may be issued when it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises." *Id.*[4]

2. The GeoFence Warrant Specified its Objects with Particularity

Under the Fourth Amendment, "a valid warrant must particularly describe the place to be searched, and the persons or things to be seized." *United States v. Kimble*, 855 F.3d 604, 610 (4th Cir. 2017) (internal quotation marks omitted). The particularity requirement constrains a warrant so that it is "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). It protects against "exploratory rummaging in a person's belongings." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (quoting *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)). Moreover, the test for particularity "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d

[4] *Zurcher*, which approved a warrant to search an innocent newspaper for evidence of crime, also demonstrates that the Fourth Amendment standards of probable cause and particularity govern warrants that raise significant First Amendment concerns. *See id.* at 565 ("courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search"). Here, the defendant cannot demand any exacting scrutiny of the GeoFence warrant merely because he robbed a bank near a church, because Fourth Amendment rights may not be vicariously asserted. *See Rakas*, 439 U.S. at 133-34. In any event, the GeoFence warrant satisfied the Fourth Amendment under the standards of *Zurcher* because it was issued based on probable cause and specified its objects with particularity.

743, 745 (8th Cir. 1976)).

Here, the GeoFence warrant was narrowly constrained based on location, dates, and times. The warrant sought only location and identity information from Google regarding a two-hour interval for individuals present at the site of a robbery during a one-hour interval. Based on the facts and circumstances investigators knew about the robbery, it was appropriately tailored toward its investigatory purpose, which was to obtain evidence to help identify and convict the armed robber.

The cell tower dump opinion *United States v. James* provides persuasive authority that the warrant here was sufficiently particular. In *James*, the defendant argued that the tower dump warrants used to identify him as a robber were insufficiently particular because they "allowed law enforcement to identify the location of hundreds if not thousands of cell phone users on specific days during specific time frames." *James*, 2019 WL 325231 at *3. The district court, however, found that the warrants were sufficiently particular because they sought information that was "constrained—both geographically and temporally—to the robberies under investigation." *Id.* This reasoning is fully applicable here: the GeoFence warrant was appropriately constrained in space and time to obtain evidence of the robbery. Indeed, the location information obtained from Google was more narrowly constrained than the location information in *James*. The 150-meter radius of the GeoFence warrant is smaller than most cellular sites, and the government only obtained location information regarding 19 individuals, rather than hundreds or thousands.

The defendant also challenges the warrant because it included the three-step process for executing the warrant that allowed investigators to obtain less than the maximum quantity of location and identity information that the warrant authorized. *See* ECF No. 29 at 24 ("The warrant left everything up to the discretion of the executing officers."). The warrant, however, established

probable cause for all the evidence that law enforcement could have obtained: identity information and two hours of location data for all individuals present at the site of the robbery during the hour of the robbery. The information specified by a warrant must be "no broader than the probable cause on which it is based," *Hurwitz*, 459 F.3d at 473, but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. Rather than violating the Fourth Amendment, the three-step process allowed investigators to further protect privacy.

The most-heavily litigated search warrant in history—the search warrant in the investigation of the Playpen child pornography website—included a similar component that allowed investigators to prioritize the evidence they seized, and courts have agreed that that component did not violate the Fourth Amendment.[5] Playpen was a dark web child pornography site with over 158,000 members. *See United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018). FBI investigators obtained a warrant authorizing a search of the computers of everyone who logged into Playpen for 30 days. *See id.* at 689. The attached affidavit, however, allowed the FBI to choose to obtain less than the maximum amount of information the warrant authorized. It explained that that "in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users." *United States v. Anzalone*, 208 F. Supp. 3d 358, 363 (D. Mass. 2016).

[5] Eleven Courts of Appeals have considered various challenges to the Playpen warrant, and all have ultimately rejected suppression. *See United States v. Taylor*, 935 F.3d 1279, 1281 (11th Cir. 2019) ("[W]e become today the eleventh (!) court of appeals to assess the constitutionality of the so-called 'NIT warrant.' Although the ten others haven't all employed the same analysis, they've all reached the same conclusion—namely, that evidence discovered under the NIT warrant need not be suppressed."). Approximately 100 district court cases have resolved suppression motions challenging the Playpen warrant. As discussed in Section III below, the Fourth Circuit rejected a challenge to the particularity of the Playpen warrant based on the good-faith exception. *See United States v. McLamb*, 880 F.3d 685, 689-91 (4th Cir. 2018).

Some defendants argued that the discretion given the FBI in executing the Playpen warrant violated the Fourth Amendment's particularity requirement, but courts uniformly rejected this argument. For example, in *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016), the court concluded that "the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site." *See also Anzalone*, 208 F. Supp. 3d at 368 ("Every court to consider this question has found the NIT search warrant sufficiently particular."). Similarly, the fact that investigators here could have and did narrow the information obtained from Google is immaterial, as the GeoFence warrant was based on probable cause and appropriately authorized seizure of location and identity information of anyone at the site of the robbery. The GeoFence warrant was not a general warrant, and this Court should deny the defendant's motion to suppress.

Finally, even if there were a particularity problem in the three-step process for the GeoFence warrant, the appropriate remedy would at most be to sever the second step of the warrant and to suppress second-step information. "[E]very federal court to consider the issue has adopted the doctrine of severance, whereby valid portions of a warrant are severed from the invalid portions and only materials seized under the authority of the valid portions, or lawfully seized while executing the valid portions, are admissible." *United States v. Sells*, 463 F.3d 1148, 1154–55 (10th Cir. 2006); *see also United States v. Jones*, 2018 WL 935396, at *16–*18 (E.D. Va. Feb. 19, 2014) (discussing and applying doctrine of severance).

Here, the first step of the GeoFence warrant targeted narrow and clearly-defined information: anonymized location information for devices within 150 meters of the bank during the hour of the robbery. Even if this Court were to find the second step to be constitutionally

inadequate, the appropriate remedy would thus be to sever the second step and retain the first.[6] Importantly, first-step information alone was sufficient for investigators to recognize that the Chatrie Account likely belonged to the robber: the defendant's electronic device was near the church prior to the robbery, inside the credit union during the robbery, and left immediately following the robbery via the area near the church. Thus, even if this Court were to sever the warrant and suppress second-step information from Google, the subsequent investigation of the defendant would not be the fruit of the poisonous tree.

C. Evidence from the GeoFence Warrant Should Not Be Suppressed Because Investigators Relied upon it in Good Faith

Even assuming the GeoFence warrant was lacking in probable cause or particularity, suppression would not be an appropriate remedy. Suppression is a remedy of "last resort," to be used for the "sole purpose" of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression "outweigh its heavy costs." *Davis v. United States*, 564 U.S. 229, 236-37 (2011). "The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144.

Search warrants for Google information about the location of its users are a new investigative technique, and there are no judicial opinions analyzing them under the Fourth Amendment. In *McLamb*, the Fourth Circuit rejected suppression in this circumstance. The court

[6] Under *Bynum*, 604 F.3d at 164, the defendant lacks a reasonable expectation of privacy in subscriber information obtained under step three of the GeoFence warrant, and he therefore lacks standing to challenge that portion of the warrant.

held that when considering a motion to suppress the fruits of a novel investigative technique, suppression was inappropriate where the investigating officer consulted with counsel and then sought a warrant:

> But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what Leon's 'good faith' expects of law enforcement. We are disinclined to conclude that a warrant is 'facially deficient' where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

McLamb, 880 F.3d at 691. Here, Task Force Officer Hylton followed the approach endorsed by *McLamb*. He had consulted with prosecutors—both state and federal—about GeoFence warrants, and he had previously obtained a similar warrant for Google location information issued by a United States Magistrate Judge. In this investigation, he then sought and obtained a search warrant from a state magistrate. Task Force Officer Hylton thus did "precisely" what *McLamb* expects, and the good-faith exception precludes suppression here.

Alternatively, the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984), leads to the same result: no suppression. When police act in "objectively reasonable reliance on a subsequently invalidated search warrant" obtained from a neutral magistrate, "the marginal or nonexistent benefits produced by suppressing evidence … cannot justify the substantial costs of exclusion." *Id.* at 922. *Leon* identified four circumstances in which an officer's reliance on a warrant would not be objectively reasonable:

> (1) when the issuing judge "was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) when "the issuing magistrate wholly abandoned his judicial role …"; (3) when "an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) when "a warrant [is] so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."

United States v. Perez, 393 F.3d 457, 461 (4th Cir. 2004) (quoting *Leon*, 468 U.S. at 923). None of these circumstances are present in this case, and the defendant does not claim that the affiant misled the magistrate or that the magistrate abandoned his judicial role.

The defendant argues that the good faith exception does not apply here because the affidavit was so lacking in indicia of probable cause that reliance on it was unreasonable, *see* ECF No. 29 at 24-25, but he is mistaken. As an initial matter, "the threshold for establishing this exception is a high one" because "[o]fficers executing warrants are not often expected to question the conclusions of an issuing authority." *United States v. Seerden*, 916 F.3d 360, 367 (4th Cir. 2019) (quoting *Messerschmidt*, 565 U.S. at 547). The defendant asserts that there was "no evidence that the robber had ever used Google," ECF No. 29 at 24-25, but he ignores that the affidavit established that the armed robber had a cell phone, that most cell phones are smartphones, and that nearly every Android phone user and some non-Android phone users use Google. Based on these facts, the executing officers' belief that the warrant to Google was issued based on probable cause was not entirely unreasonable, and the good faith exception thus precludes suppression.

The defendant also argues that the good faith exception does not apply because the warrant was so facially deficient in failing to specify the things to be seized that officers could not reasonably rely on it. *See* ECF No. 29 at 24. But as discussed in Section II.B above, the warrant was quite specific in scope: it was limited to anonymized location information over a two-hour interval, as well as accompanying identity information for a smaller subset, for individuals present at the site of the robbery during a one-hour interval.

In addition, the defendant argues that the warrant was facially deficient because it allowed officers to choose to obtain less information about those present at the robbery, *see* ECF No. 29 at 25, but this argument is foreclosed by *McLamb*. The defendant in *McLamb* argued to the Fourth

Circuit that the Playpen warrant was insufficiently particular, in part because it allowed the FBI to "deploy the [search technique] more discretely against particular users." *See* Brief of Appellant at 46-47, *United States v. McLamb*, No. 17-4299 (available at 2017 WL 2832704). The Fourth Circuit relied on *Leon*'s good-faith exception to reject suppression, concluding that the Playpen warrant was not "so 'facially deficient ... that the executing officers [could not] reasonably presume it to be valid.'" *McLamb*, 880 F.3d at 691. The warrant thus was not facially deficient, and this Court should deny the defendant's motion to suppress.

III. CONCLUSION

For the reasons set forth in this brief, this Court should deny the defendant's motion to suppress the fruits of the GeoFence warrant.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Office of the United States Attorney
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 19th day of November, 2019, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koenig
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorney
Office of the United States Attorney
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

DEFENDANT'S REPLY TO GOVERNMENT'S RESPONSE MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A "GEOFENCE" GENERAL WARRANT

Okello Chatrie, through counsel, replies as follows to the government's response to his motion to suppress evidence obtained from a "geofence" general warrant. *See* ECF No. 29.

I. Obtaining Mr. Chatrie's Google location information was a search.

Mr. Chatrie presents two arguments as to why the government's acquisition of his Google location data was a search. The government responds to only one of them on the merits. First, Mr. Chatrie argues that the government's conduct was a search under the *Katz* reasonable expectation of privacy test. The government contends that he had no privacy interest in two hours of his location information, failing to appreciate the significance of the Supreme Court's landmark decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and seeking to create a *de minimis* exception to the Fourth Amendment. Second, Mr. Chatrie argues that it was a search under a property rights theory of the Fourth Amendment. This understanding of the Fourth Amendment predates *United States v. Katz*, 389 U.S. 347 (1967), and has been repeatedly identified by the Supreme Court as an equally valid and independent test. *See, e.g.*, *United States v. Jones*, 565 U.S. 400, 409 (2012); *Kyllo v. United States*, 533 U.S. 27, 37 (2001); *Soldal v. Cook County*, 506 U.S. 56, 62 (1992). The government, however, brushes it aside as if it were a recent invention of Justice

Gorsuch, offering no response on the merits. ECF No. 41 at 12. Under both theories, however, the acquisition of Mr. Chatrie's Google location data was a search.

A. Obtaining Mr. Chatrie's Google location information infringed on his reasonable expectation of privacy.

The government contends that Mr. Chatrie had "no reasonable expectation of privacy in any of the information disclosed by Google" because the location data covered two hours instead of seven days. ECF No. 41 at 6. But *Carpenter* did not gift the government a free pass from the Fourth Amendment for any such "limited period." 138 S. Ct. at 2220. On the contrary, the Court made it clear that it would not "grant the state unrestricted access to a wireless carrier's database of physical location information," describing such information as "deeply revealing," "comprehensive," and "inescapable" *Id.* at 2223. Mr. Chatrie had a reasonable expectation of privacy in his Google location information, which was at least as private as the records in *Carpenter*.

Carpenter involved two orders for historical cell site location information ("CSLI"): one seeking 152 days, and a second for seven days. 138 S. Ct. at 2212. In holding that a warrant is required for seven days or more of CSLI, the Court merely decided *Carpenter* on the facts before it. There is no higher constitutional significance to seven days, and *Carpenter* does not suggest that the Fourth Amendment would condone warrantless searches for a shorter period of time. In fact, the second CSLI order only produced only two days of records, not seven. *Id.* at 2212. Likewise, the Court did not express a view on real-time CSLI or "tower dumps" because those facts were not present in the record. *Id.* at 2220. But it would require misreading the rest of the Court's opinion to view this judicial restraint as an invitation to engage in warrantless surveillance. It is not enough to suppose, as the government does, that it might be possible to replicate this

location information given enough time and resources.[1] ECF No. 41 at 8. While some physical searches may be permissible without a warrant, the Court has been clear that "any extension of that reasoning to digital data has to rest on its own bottom." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

Applying the *Carpenter* framework, it is clear that obtaining Google location data was a search that infringed on Mr. Chatrie's reasonable expectation of privacy. Like the CSLI in *Carpenter*, Google location information is deeply revealing, comprehensive, and inescapable. 138 S. Ct. at 2223. It its revealing because it can expose the location of devices inside constitutionally protected areas, including "private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* at 2218. Indeed, Google uses it for that very purpose when serving advertisements. Google Policies, Location Data (Nov. 20, 2018), https://policies.google.com/technologies/location-data?hl=en. And in this case, it located 11 users inside the Journey Christian Church, a quintessentially protected space that raises additional First Amendment concerns. *See Stanford v. Texas*, 379 U.S. 476, 485 (1965) (requiring courts to apply Fourth Amendment requirements with "the most scrupulous exactitude" when searches implicate First Amendment concerns).[2] In sum, two hours of Google location information is capable of revealing the same type of sensitive, private information as CLSI.

[1] Mr. Chatrie maintains that the data obtained through this warrant could not have been obtained through visual surveillance alone. In addition to subscriber information and account details, which are not observable, it would have been impossible to reconstruct all of the location data obtained from Google. Even if the government had unlimited time and resources, they would not be free to enter constitutionally protected spaces to log the devices located inside. Mr. Chatrie does not concede his privacy interest in the non-location data obtained through the geofence warrant.

[2] The government fails to adequately address these First Amendment concerns, just as it failed to recognize or address them when seeking a geofence warrant that fully encompassed a large church. The affiant simply described the church as "an adjacent business" without telling the Court that the "business" was actually a church.

The fact that the government obtained a smaller quantity of this location data than in *Carpenter* does not diminish its potentially revealing nature. *Carpenter* emphasized the long-term privacy implications of cell phone location tracking only because those were the facts before the Court. Elsewhere, the Justices have expressed concern with even short-term monitoring. In *United States v. Karo*, for example, the use of a beeper to track a drum of ether inside a private residence was sufficient to trigger Fourth Amendment scrutiny. 468 U.S. 705, 716 (1984) ("We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device . . . whether a particular article—or a person, for that matter—is in an individual's home *at a particular time*.") (emphasis added). Just a small window of GPS monitoring still creates a "precise, comprehensive record of a person's movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). Indeed, it takes little imagination to conjure the privacy implications of even a single trip to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Id.* (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-442 (2009)).

Far more troubling is the breadth of the search in this case. Whereas *Carpenter* concerned the search of just one person's location data, the geofence warrant authorized the search of an unlimited number of people's location data. Neither the government nor the magistrate knew in advance how many devices would be swept up as a result of the search. Indeed, the fact that it would yield information about 19 different devices was unknowable at the time of the government's application. This was not a problem the *Carpenter* Court had occasion to consider,

but it is one that has repeatedly troubled the Court.[3] Indeed, "dragnet" searches are a perennial Fourth Amendment fear. That is why the Constitution prohibits general warrants and requires both probable cause and sufficient particularity. Even if obtaining two hours of location data for a single person would not trouble the Court, obtaining two hours of data for every person in an area is a very different story. In this sense, it arouses the same fears of "too permeating police surveillance" and exercise of "arbitrary power" that motivated the *Carpenter* Court. 138 S. Ct. at 2214. Although the concerns in *Carpenter* are not identical, the potentially unlimited breadth of a geofence search makes up for the comparatively shorter duration of a geofence search. Consequently, the data obtained are highly revealing and deserving of Fourth Amendment protection, as much if not more so than the CSLI in *Carpenter*.

Similarly, Google location data has a comprehensive reach that is comparable to CSLI. In fact, CSLI *is* one of the data sources that Google collects and uses to determine users' locations. But Google also includes GPS location data as well as "additional information from nearby Wi-Fi, mobile networks, and device sensors." Google Policies, *supra*. As a result, Google location information is significantly more precise than CSLI alone. The government puts no stock in this distinction because the *Carpenter* Court "t[ook] account of more sophisticated systems" and recognized that CSLI "is rapidly approaching GPS-level precision." [G. at 8-9 (quoting *Carpenter*, 138 S. C.t at 2218-19).] But because Google uses multiple sources of location data, it locates devices even in places where GPS is unavailable or unreliable, such as indoors. If GPS data is not

[3]*See, e.g.*, *United States v. Knotts*, 460 U.S. 276, 284 (1983) (reserving the question of whether "different constitutional principles may be applicable" to "dragnet-type law enforcement practices"); *see also Jones*, 565 U.S. at 408 n.6 (quoting *Knotts*); *Karo*, 468 U.S. at 716 ("Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."); *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 327 (1972) (Douglas, J., concurring) ("[T]he recurring desire of reigning officials to employ dragnet techniques … lies at the core of [the Fourth Amendment]."); *Davis v. Mississippi*, 394 U.S. 721, 726 (1969) ("Nothing is more clear than that the Fourth Amendment was meant to prevent wholesale intrusions upon the personal security of our citizenry").

available, Google will then approximate location information based on the signal strength of known nearby Wi-Fi networks, which have a short range. Google is capable of doing this by referencing the billions of data points it gathers each day from other Android phones that report on the availability of Wi-Fi networks in range. *See* Tr. at 29, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019) (Ex. D). Only when Wi-Fi and GPS are unavailable does Google fall back to using CSLI, the least precise method. Consequently, Google location data is likely to be *more* comprehensive than GPS, locating devices where GPS is unavailable.

And finally, Google location data is "automatic and inescapable." For Android users like Mr. Chatrie, there is no practical way to avoid transmitting location information to Google, even if "Location History" is turned off. Location History only controls whether location data gets added to a user's "Timeline" feature, not whether Google sees or stores the data. Likewise, disabling Google Location Services does not actually stop a device from determining its location and creating a record. As Google explains, "Your device's location will continue to work even if GLS [Google Location Services] is turned off, but the device will rely only on GPS to estimate device location for apps with the necessary permission." Google Policies, *supra*. Those apps include basic, built-in Google services like Search and Maps. Thus, because "Google Location Services is distinct from your device's location setting," some location information still flows to Google even when it is off. *See* Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb. And while Google notes that there are separate controls for "Web & App Activity," this setting is isolated and unaffected by the restriction of other location information. Furthermore, the government is incorrect that Mr. Chatrie "had to affirmatively opt in" to sharing his location information with Google. As the user of an Android phone, Google Location Services is enabled

by default. *See* Verizon, Samsung Galaxy S9 / S9+ - Activate / Set Up Device, https://www.verizonwireless.com/support/knowledge-base-216675/ (showing Google location services on by default at step eight). Location History, by contrast, is an opt-in feature, but one that has no effect on the GPS, Wi-Fi, and other location data transmitted to Google through Location Services or Web & App Activity.[4] While it is technically possible to disable the phone's location functions altogether by activating "airplane mode" or powering off the device completely, such drastic steps are not required by *Carpenter*. 138 S. Ct. at 2220 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."). Rather, collection of Google location data is "inescapable" because, as in *Carpenter*, it relates to services one needs to be a functioning member of today's society. *Id*. In addition the ubiquity of Google services such as Search, Maps, and Mail, all Android phones—such as the one Mr. Chatrie had—run on Google's operating system and regularly transmit location data back to Google without any affirmative user action at all. The collection is therefore just as automatic and inescapable as CSLI.

In sum, Google location data is at least as revealing, comprehensive, and inescapable as CSLI. Thus, as in *Carpenter*, the fact that "such records are generated for commercial purposes . . . does not negate [Mr. Chatrie's] anticipation of privacy in his physical location." 138 S. Ct. at 2217. Mr. Chatrie had a reasonable expectation of privacy in his Google location data and obtaining those records was therefore a Fourth Amendment search. This is especially true because

[4] The government also draws a confusing and unsupported distinction between "incidental" disclosure of location information and disclosure as a "central prerequisite" to obtaining services. CSLI, however, is in fact essential to the use of a cell phone – required to route information to the correct tower and device. It is both central to the way cell phones function and a prerequisite to using their features.

of the "dragnet-style" search used to get them, a longstanding fear of the Court even when long-term surveillance is not at issue.

B. Obtaining Mr. Chatrie's Google location information infringed on his property rights in that data.

The *Katz* reasonable-expectation-of-privacy test has been in place since 1967, but the Supreme Court's Fourth Amendment jurisprudence is not so young. Throughout the late-19th and early-20th centuries, the Court hued closely to a literal reading of the constitutional text, focusing on the property rights attached to "persons, houses, papers, and effects." U.S. Const. amnd. IV; *see, e.g.*, *Agnello v. United States*, 269 U.S. 20, 32 (1925) ("The search of a private dwelling without a warrant is in itself unreasonable and abhorrent to our laws."); *Weeks v. United States*, 232 U.S. 383, 391 (1914) (recognizing that the essence of a Fourth Amendment violation is "the invasion of his indefeasible right of personal security, personal liberty, and private property."); *Ex parte Jackson*, 96 U.S. 727, 732-33 (1878) (holding that postal mail is just as protected under the Fourth Amendment as those papers and effects kept in the safety of one's home). Indeed, the invasion of property rights was at the heart of Lord Camden's judgment in *Entick v. Carrington*, one of the pillars of English liberty and a catalyst for the Fourth Amendment. 19 How. St. Tr. 1029 (K.B. 1765) ("Papers are the owner's goods and chattels. They are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection"); *see also Boyd v. United States*, 116 U.S. 616, 626 (1886) (describing *Entick* as a "monument of English freedom" and "the true and ultimate expression of constitutional law"). On this side of the Atlantic, the founding fathers specifically designed the Fourth Amendment to assure security "in person *and property*" against unlawful searches. *Adams v. New York*, 192 U.S. 585, 598 (1904) (emphasis added). In short, the "traditional," property-based theory of the Fourth Amendment has a pedigree that long predates *Katz* and, given the Court's recent jurisprudence, is as valid as ever.

When the Court decided *Katz*, there was a palpable worry that property rights alone would not be sufficient to implement the Fourth Amendment in an age when communications could occur without an in-person meeting, but through electronic whispers miles apart. Justice Harlan embodied this concern in his famous concurrence, declaring that the Fourth Amendment protects "people, not places." 389 U.S. at 351. This understanding of the Fourth Amendment has served the Court well for decades, but it "did not repudiate [the] understanding" held for "most of our history" that the Fourth Amendment embodies "a particular concern for government trespass" on one's "papers" and "effects." *Jones*, 565 U.S. at 406-07.

Thus, for example, the Court in *Soldal* unanimously held that removal of a tenant's mobile home was a Fourth Amendment seizure even though the owner's "privacy" was not invaded. 506 U.S. at 62 ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). Likewise, in *Kyllo*, Justice Scalia avoided the *Katz* doctrine in finding that the use of a thermal imager on a home was a search. 533 U.S. at 37 ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."). Indeed, the *Kyllo* Court noted that "well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass." *Id.* at 40. And finally, in *Jones*, the opinion of the Court rested on trespass grounds. 565 U.S. at 404-05. The *Jones* Court found that placement of a GPS tracker on a car was a "physical intrusion" that "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id*. Reaffirming *Soldal*, the *Jones* Court unequivocally stated that "the *Katz* reasonable-expectation-of-privacy test had been *added to*, not *substituted for*, the common-law trespassory test." *Id.* at 409; *see also Jones*, 565 U.S. at 414 (Sotomayor, J., concurring) ("*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.").

Justice Gorsuch's dissent in *Carpenter* was a clarion call for courts and counsel to reassert the central role that property rights have played in the history of Fourth Amendment jurisprudence. 138 S. Ct. at 2272 ("Carpenter pursued only a *Katz* 'reasonable expectations' argument. He did not invoke the law of property or any analogies to the common law, … [and therefore] forfeited perhaps his most promising line of argument."). Mr. Chatrie does not ask this Court to adopt a novel theory, but to apply a deep-rooted one. *See id.* at 406-07. Mr. Chatrie takes Justice Gorsuch's warning seriously and seeks to fully assert his Fourth Amendment rights. The government, however, simply does not engage with the merits of Mr. Chatrie's property-based argument. ECF No. 41 at 12-13. Instead, the government chooses to ignore over a century of Fourth Amendment jurisprudence and merely quip that "a solo dissent is not the law." *Id.* at 12.

II. The warrant lacked probable cause and was even more unparticularized than previously thought.

The government responds that the geofence warrant was supported by sufficient probable cause and particularity. *Id.* at 13-21. But their arguments are even less persuasive in light of additional discovery showing that they twice requested additional location data on all 19 devices initially identified by Google, in contravention of the warrant itself. *See* Ex. A (First Step 2 Request) at 1; Ex. B (Second Step 2 Request) at 1. Indeed, Google twice rebuffed this request, ultimately sending additional information on nine devices. This development underscores why such an ad hoc, back-and-forth negotiation with the recipient of a warrant is no substitute for judicial oversight and a particularized warrant supported by probable cause.

More fundamentally, the government's response appears to misunderstand the significance of the Fourth Amendment's particularity requirement. Particularity is not just about how clearly a warrant identifies the object of a search for which there is probable cause to seize, but whether it adequately constrains law enforcement's discretion in the execution of that search and seizure. Its

basic purpose is to prevent general warrants by ensuring that "nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). The government contends that the information it sought was "constrained" based on location, date, and time to the robbery under investigation. ECF No. 41 at 18. But it is not enough to simply name the crime and identify the general area where it occurred. Rather, such a warrant is more akin to the general warrant in *Wilkes v. Wood* that identified the crime of seditious libel but did not specify the places to be searched, the papers to be seized, or the persons to arrest. 98 Eng. Rep. 489, 490 (1763). Drawing a circle around the neighborhood to be ransacked does not change the analysis.

The government contends that the initial search ("Step One") satisfied the particularity and probable cause requirements because it specified information "directly tied" to a particular robbery, which of course occurred "at a particular place and time." ECF No. 41 at 13. But it failed to individualize its suspicion and tie that robbery to a particular account or accounts to be searched. That is like permitting the police to search for stolen goods in any place near a theft, to pat down every person in a bar where a crime had been committed, or to search every person in an apartment where illegal drugs may be present--all of which courts have found to be unconstitutional. *See Grumon v. Raymond*, 1 Conn. 40, 43 (1814); *United States v. Glenn*, *2009 WL 2390353*, at *5 (S.D. Ga. 2009); *Commonwealth v. Brown*, 68 Mass. App. Ct. 261, 262 (Mass. App. Ct. 2007). It is also strongly reminiscent of the facts in *United States v. Curry*, in which this Court held that police did not have reasonable suspicion to stop Mr. Curry or any of the other men in a group after shots were fired in the general vicinity of where he was walking. No. 3:17CR130, 2018 WL 1384298, at *11 (E.D. Va. Mar. 19, 2018), *rev'd and remanded*, 937 F.3d 363 (4th Cir. 2019), *reh'g en banc granted*, No. 18-4233, 2019 WL 6133704 (4th Cir. Nov. 18, 2019) ("[G]eneralized suspicion and fear cannot substitute for specific and articulable facts . . . that support a

particularized and objective basis for suspecting *the particular person stopped* of criminal activity.") (internal quotations omitted). The government scoffs at the fact that "19 individuals, rather than hundreds or thousands" were affected by Step One of the warrant, ECF No. 41 at 18, but it gives no indication of how many bystanders would have to be searched before the collateral damage becomes too much for the Fourth Amendment to bear. Indeed, the government did not and could not have known how many devices would be affected by such a high-tech fishing expedition. The only thing certain at Step One was that law enforcement intended to search the Google data of many people who were *not* involved in the robbery.

It is not sufficient to respond, as the government does, that the location records of admittedly innocent people are the proper target of a search warrant on the off-chance that they might be useful in reconstructing the scene, identifying potential witnesses, or rebutting potential defenses raised by the robber. ECF No. 41 at 16. This argument proves too much. The issue is not whether there is some evidence to be had, but where the line is between a general warrant and a particularized one. The boilerplate speculation offered by the government would seemingly justify a search of anyone near any crime.

Moreover, the underlying reason the warrant lacks particularity is because the government does not have probable cause to search an unlimited number of unknown people who were near a crime. Probable cause is what makes particularity possible. Without it, there should be no surprise when a warrant also lacks particularity. As the government notes, the "information specified by a warrant must be 'no broader than the probable cause on which it is based.'" ECF No. 41 at 19 (citing *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006)). But here, the distinguishing feature of the warrant application is the absence of any identifiable suspects. Without some

individualized suspicion, it is trying to imagine how the resulting warrant would be anything other than unparticularized.

Contrary to the government's assertion, the warrant application established no probable cause for any of the Google data it obtained. Mere proximity to crime is not probable cause of criminal activity. The government points to the so-called "Playpen warrant" as precedent for its actions here, *Id.* at 20, but unlike the Playpen cases, there was no honeypot in this case—only a dragnet. The Playpen warrant was "based on probable cause to search any computer logging into [a child pornography website]." *Id.* at 20 (quoting *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016)). The suspicion generated as a result of logging in to such a website has been a critical element in decisions upholding that warrant's constitutionality. See, e.g., *Matish*, 193 F. Supp. 3d at 603 (finding that the "chances of someone innocently discovering, registering for, and entering Playpen were slim" because of the "numerous affirmative steps that one must take to even find Playpen on the Tor network" that make it "extremely unlikely for someone to stumble innocently upon Playpen"); *see also United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018) (noting that to access Playpen, a user must download Tor and enter a 16-character URL consisting of random letters and numbers, as well as enter a username and password to proceed past a welcome page that "was suggestive enough that Playpen's content would be apparent" to any visitor). In this case, however, there is no argument that using Google services or being near the Call Federal Credit Union is somehow inherently suspicious. Instead, a crime was committed, law enforcement had no suspects, and the government simply cast a dragnet. The prevalence of Android phones is not probable cause to search any Google users that happen to be nearby. And

the absence of any individualized suspicion, let alone probable cause, at Step One renders the entire warrant unconstitutional.[5]

The second phase of the warrant ("Step Two") fares even worse. The government asserts that the warrant was "remarkably limited" because it obtained the location information for nine individuals over a two-hour interval, regardless of whether they were inside or outside the 150-meter radius. ECF No. 41 at 13. Indeed, the government commends itself for seizing "less than the maximum quantity of location and identity information that the warrant authorized." ECF No. 41 at 18. But this argument only gives lie to the entire three-step process. According to the government, the warrant authorized the government to seize "identity information and two hours of location data for *all individuals* present at the site of the robbery during the hour of the robbery." *Id.* at 19 (emphasis added). The warrant, however, is not so clear on this point.

The impression one gets from reading the warrant application is that the three-step process matters—that it is a means of protecting the privacy of bystanders by using "anonymized"[6] data to "narrow down the list" before obtaining additional records in Step Two, and then de-anonymized identity information in the third phase ("Step Three"). But the government, in its requests to Google and in a careful reading of Attachment II, said that they were actually entitled to Step 2 and Step 3 data on *everyone* snared in Step 1, no narrowing required. The warrant only says that law enforcement will "attempt" to narrow the list in Steps 2 and 3. *See* Warrant

[5] The government invites this Court to "sever the second step of the warrant and to suppress second-step information" only, ECF No. 41 at 20, but to do so would condone the digital equivalent of a general warrant that lacked particularity from the outset. *See, e.g., United States v. Sells*, 463 F.3d 1148, 1158 (10th Cir. 2006) (noting that "every court to adopt the severance doctrine has further limited its application to prohibit severance from saving a warrant that has been rendered a general warrant by nature of its invalid portions despite containing some valid portion").
[6] Mr. Chatrie does not concede that this data is not personally identifiable.

Attachment I at 1-2; Warrant Attachment II at 2-3. The verb "attempt" appears six times, doing quite a lot of work.

The government did in fact request the "maximum" amount of data—twice. In two emails to Google following the production of Stage One records, the government asked for "additional location data and subscriber info" for all 19 devices identified in step one. *See* Ex. A at 1; Ex. B at 1. Google did not respond to either of these requests. It was not until the government sent a third email requesting additional data on just nine devices that Google produced more records. *See* Ex. C (Third Step 2 Request) at 1. This is not to suggest that the government did not "attempt" to narrow down the list. Indeed, the government twice tells Google, "If this request seems unreasonable, please keep in mind that device numbers 1-9 may fit the more likely profile of parties involved," but then requested additional information on all 19 anyway. *See* Ex. A at 1; Ex. B at 1.

It is unclear whether the practical realties of the three-step process were apparent to the issuing magistrate. It was certainly not clear to Mr. Chatrie prior to reviewing the negotiations between Google and law enforcement over the data to be produced in Step Two. The critical point, however, is that it was up to Google to decide whether the additional search was "reasonable." *Id.* That is a question that the Constitution makes clear is for a neutral and detached magistrate, not Google. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004) ("Even though [law enforcement] acted with restraint in conducting the search, 'the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.'") (quoting *Katz*, 389 U.S. at 356). In reality, the government would have obtained the "maximum" amount of data authorized had Google not enforced the warrant's strong suggestion that law enforcement should be required to first "narrow down the list." *See* Ex. A at 1; Ex. B at 1. Google, not the government, deserves commendation

for somewhat limiting the scope of this dragnet search—but it is not and should not be their job to do so.

Put simply, the government lacked probable cause to search any individual's location data, so law enforcement sought to search a broad swath of everyone's data in the area of the robbery. Without sufficient probable cause, the warrant was doomed from the start, as further evinced by its equal lack of particularity. The government's "attempt" to "narrow down the list" was merely cosmetic, masking its multiple grabs for the "maximum" amount of data that it believed investigators was entitled to. Law enforcement's emails to Google clearly demonstrate how the government viewed the three-step process as no more than window dressing. Instead, the government put Google in the role of magistrate, deferring to Silicon Valley to determine what was "reasonable." *See* Ex. A at 1; Ex. B at 1. Such a delegation of constitutional authority is contrary to the Fourth Amendment, demonstrating the profound absence of probable cause or particularity in this case.

III. The warrant was *void ab initio*.

The government seeks to sidestep the unlimited breadth of the warrant by arguing that Mr. Chatrie "lacks standing to challenge the government's acquisition of others' location information." ECF No. 41 at 12. But Mr. Chatrie is not asserting the Fourth Amendment rights of others; he is asserting his own. The unlimited breadth of the warrant bears directly on its absence of particularity, rendering it an unconstitutional general warrant that was *void ab initio*—invalid from the beginning. *See Groh*, 540 U.S. at 558 (finding a warrant "so obviously deficient" in particularity that "we must regard the search as 'warrantless' within the meaning of our case law.").

The history of the Fourth Amendment and the framers of the Constitution make this very clear. For example, "[w]hen James Otis, Jr., delivered his courtroom oration against writs of

assistance in 1761," he argued that "the writs … were void as a form of general warrant." *Payton v. New York*, 445 U.S. 573, 608 (1980) (White, J., dissenting). Lord Camden's judgment in *Entick*, one of the pillars of English liberty and a catalyst for the Fourth Amendment, similarly held a general warrant to be "illegal and void." 19 How. St. Tr. 1029; *see Boyd*, 116 U.S. at 616 (citing this holding and noting that "the principles laid down in [*Entick*] affect the very essence of constitutional liberty and security."); *State Tax Comm'n v. Tenn. Coal, Iron & R. Co.*, 89 So. 179, 182 (Ala. 1921) (noting *Entick*'s holding that "the general warrants issued by the Secretary of State were, under such circumstances there outlined, declared illegal and void."). And when a warrant is void, "potential questions of 'harmlessness'" do not matter. *United States v. Krueger*, 809 F.3d 1109, 1123 (10th Cir. 2015) (Gorsuch, J., concurring). The geofence warrant violated Mr. Chatrie's Fourth Amendment rights, not just the rights of bystanders.

IV. The good faith doctrine does not apply.

The *Leon* good faith exception to the exclusionary rule does not apply to evidence discovered as a result of an arrest premised upon a warrant that was *void ab initio*. As the *Leon* Court explained, "in so limiting the suppression remedy, we leave untouched the probable-cause standard and the various requirements for a valid warrant." 468 U.S. 897, 923-24 (1984). Thus, the good-faith exception is inapplicable to warrants that do not meet the probable cause and particularity requirements. While the Fourth Circuit has applied the good faith exception to warrants authorized by magistrates lacking jurisdiction, *McLamb*, 880 F.3d at 691, the Circuit did so because suppression would not have appreciably deterred police misconduct. *See United States v. Seerden*, 916 F.3d 360, 367 (4th Cir. 2019). By contrast, the Fourth Circuit has never applied the good faith doctrine to a general warrant, as suppression serves the goal of deterring police from seeking such intentionally overbroad and unparticularized warrants in the future. *Leon* may excuse

a deficiency in the language of a warrant that is subsequently invalidated, but it cannot excuse a general warrant that is void at its inception. To hold otherwise would incentivize the kind of "systemic error" and "reckless disregard of constitutional requirements" that the Supreme Court has cautioned against. *Herring v. United States*, 555 U.S. 135, 144 (2009).

Even if *Leon* were to apply in this case, evidence from an unconstitutional search should still be suppressed in at least four circumstances, three of which are relevant here. *See United States v. Leon*, 468 U.S. 897, 923 (1984).

First, magistrate issuing the geofence warrant "abandoned his judicial role" by granting immense discretion to the executing officers to decide what Google data to search, and so "no reasonably well trained officer should [have] rel[ied] on the warrant." *See id.* (citing *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319 (1979)). *Lo-Ji Sales* determined that a "Town Justice" abandoned his judicial role when he accompanied the police to execute a warrant for obscene material at a store and granted the police immense discretion in seizing materials. 442 U.S. at 326-27. "When he ordered an item seized because he believed it was obscene, he instructed the police officers to seize all 'similar' items as well, leaving determination of what was 'similar' to the officer's [sic] discretion." *Id.* at 327. "The Fourth Amendment does not permit such action," nor such "open-ended warrants." *Id.* at 325. Among other problems, this grant of discretion prevents the magistrate from "verify[ing] that the inventory prepared by the police . . . accurately reflected what he had ordered seized." *Id.* at 327. Here, the warrant left it up to law enforcement and Google to decide which devices would be subject to further search in Steps 2 and 3. "The Fourth Amendment does not permit such action," reserving this function for the judiciary. *See id.* at 325. Here, the court would have no way of determining whether the data obtained in Steps 2 and 3 "accurately reflected" what the magistrate had ordered seized because there were no separate court orders

authorizing them. Instead, it was effectively an "open-ended warrant," *id.*, in which the magistrate abandoned his judicial role.

Second, the good faith exception should not apply because the government's generalized assumptions about cell phone use rendered the geofence warrant "so lacking in indicia of probable cause" to search Mr. Chatrie's data that "official belief in its existence [was] entirely unreasonable." *See Leon*, 468 U.S. at 923 (internal citations and quotations omitted). In *United States v. Doyle*, for example, the Fourth Circuit Court of Appeals held that good faith did not apply when the police searched a house for child pornography with a warrant that contained "remarkably scant evidence … to support a belief that [the defendant] *in fact* possessed child pornography." 650 F.3d 460, 472 (2011) (emphasis added). The district court incorrectly "opined that '[t]he magistrate could reasonably infer'" this possession from the affidavit's recitation of allegations of sexual assault by children and second-hand allegations of possession of child pornography. *Id.* at 471-72. In *Seerden*, by contrast, good faith did apply where the affidavit contained allegations and admissions of the actual crime for which evidence was sought (sexual assault). 916 F.3d 360, 367-68 (4th Cir. 2019). Here, the police presented no evidence that the robber "in fact" had a smartphone, used Android or Google services, and opted-in to location services, and thus that his data was "in fact" in Google's Sensorvault. *See Doyle*, 650 F.3d at 472; ECF No. 41 at 14. Per *Doyle*, this Court cannot "reasonably infer" this fact from the government's generalized assumptions about cell phone use and should instead hold that any "belief in [the] existence [of probable cause for the warrant was] entirely unreasonable." *See Doyle*, 650 F.3d at 471; *see Leon*, 468 U.S. at 923.

Third, good faith should not apply because the geofence warrant was "facially deficient." *See Leon*, 468 U.S. at 923. It sought unfettered discretion to search deeply private data of an

unlimited number of people, and was so lacking in probable cause and particularity that "the executing officers [could not have] reasonably presume[d] it to be valid." *See id*. The government's attempt to evade this problem with *McLamb* is unpersuasive. In *McLamb*, the court found that "the boundaries of a magistrate judge's jurisdiction in the context of remote access warrant" was not clear at the time the agent applied for the warrant. 880 F.3d at 691. In those very limited circumstances, the court looked to the agent's consultation with attorneys from a specialized section within DOJ as evidence of good faith. Here, the watershed decision in *Carpenter* provided significant guidance for officers in this case. This Court cannot allow a reference to consulting with a government attorney to subsume the Fourth Amendment's requirement that a neutral and detached magistrate decide whether to issue the warrant.

As the Supreme Court recognized many decades ago, the Fourth Amendment requires a "neutral and detached" judge to find probable cause because the investigating officers are engaged in "the often competitive enterprise of ferreting out crime." *Coolidge v. New Hampshire*, 403 U.S. 443, 449 (1971). "[T]he whole point of the basic rule . . . is that prosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own investigations—the 'competitive enterprise' that must rightly engage their single-minded attention." *Id.* at 450. Thus, it is the role of only the courts to enforce the constitutional requirement of particularity. To adopt the government's position here that consulting with members of the prosecution team is sufficient to establish good faith would completely eviscerate a clear protection that the Fourth Amendment in its own words requires.

CONCLUSION

The geofence warrant in this case was a general warrant, devoid of the probable cause and particularity required by the Fourth Amendment, the unconstitutionality of which should have been

readily apparent. For the foregoing reasons, Mr. Chatrie requests that this Court find the warrant void and suppress all of the fruits thereof.

Respectfully submitted,

OKELLO T. CHATRIE

By: _____/s/_____

Michael W. Price
NY Bar No. 4771697 (pro hac vice)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on December 9, 2019, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

/s/

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]
[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472
Importance: High

Google Legal Team,

I'm writing to inquire about my correspondence with your office on 07/01 and 07/02. Please keep in mind that expedition is requested based on armed and dangerous subject(s) still being at large. Subject was on cell phone just prior to violent act; therefore, Google may have captured pertinent information to identify and arrest parties involved. See below:

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

As discussed yesterday over the phone, I appreciate your quick response and willingness to provide GPS data for the below device ID(s). Please expedite this request where possible due to this suspect's continued threat to our community. If it would speed up the process, please provide data as it becomes accessible/available, starting with device ID(s) 1 – 9. It was mentioned that the larger the request, the more time it will take to get data back. With this in mind, I will still have to rule out device ID(s) 1-9; however, I may be able to do so more quickly if I can begin reviewing data. The faster I can review the data, the faster I can get this guy/guys off the street.

Thanks again for your professionalism and understanding. I realize that I'm asking for a lot and you and your team are likely tasked-out already, but any and all assistance and expedited process is MUCH appreciated.

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

[redacted]

"If you only do what you can do, you will never be better than what you are now."

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

GOVERNMENT'S NOTICE REGARDING ATTACHMENT OF GOOGLE GEOFENCE STATE SEARCH WARRANT TO RESPONSE IN OPPOSITION TO MOTION TO SUPPRESS

The United States of America, by its undersigned attorneys, hereby provides notice that the State Search Warrant attached to this Notice is the underlying search warrant relevant to the Defendant's Motion to Suppress Evidence Obtained from the Google "Geofence" Search Warrant, the United States' Response in Opposition, and the Defendant's Reply. ECF Nos. 29, 41, 48. Accordingly, the United States seeks to have the attached search warrant docketed as an exhibit to its Response in Opposition to the Defendant's Motion. *See* ECF No. 41.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
United States Attorney's Office
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 18th day of December, 2019, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koenig
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

ALL INFORMATION SEALED

USCA4 Appeal: 22-4489 Doc: 19-1 Filed: 01/20/2023 Pg: 115 of 184Total Pages:(115 of 2164)

J.A. 107

AFFIDAVIT FOR SEARCH WARRANT

Commonwealth of Virginia VA. CODE § 19.2-54

The undersigned Applicant states under oath:

1. A search is requested in relation to [X] an offense substantially described as follows:
   [ ] a person to be arrested for whom a warrant or process for arrest has been issued identified as follows:

   Code of Virginia 18.2-58: Robbery
   Code of Virginia 18.2-53.1: Use of a Firearm in Commission of a Felony

[ ] CONTINUED ON ATTACHED SHEET

2. The place, person or thing to be searched is described as follows:

   Google LLC, which is headquartered at 1600 Google Amphitheater Parkway, Mountain View, California 94043, and applies to Target Location: Geographical area pertaining to a radius of 150 meters around a latitude/longitude coordinate, Latitude: 37.438420, Longitude: -77.587900. It is your affiant's belief that the records requested are actually possessed by Google LLC, and that Google LLC provides electronic communication service or remote computing service within the Commonwealth of VA. (See Attachment I. for Additional Information)

[ ] CONTINUED ON ATTACHED SHEET

3. The things or persons to be searched for are described as follows:

   See Attachment II.

2019 JUN 14 AM 10:30

[ ] CONTINUED ON ATTACHED SHEET

(OVER)

FORM DC-338 (MASTER, PAGE ONE OF TWO) 07/17

FILE NO. 744

AFFIDAVIT FOR SEARCH WARRANT

APPLICANT:

J.P. Hylton
NAME

Master Detective
TITLE (IF ANY)

P.O. Box 148
ADDRESS

Chesterfield, VA 23832

Certified to Clerk of Chesterfield Circuit Court
CITY OR COUNTY

on 6/14/19
DATE

Magistrate
TITLE

David Bailey
SIGNATURE

Original Delivered [X] in person [ ] by certified mail
[X] by electronically transmitted facsimile
[ ] by use of filing/security procedures defined in the Uniform Electronic Transactions Act

to Clerk of Chesterfield Circuit Court
CITY OR COUNTY WHERE EXECUTED

on 6/14/19
DATE

Magistrate
TITLE

David Bailey
SIGNATURE

USCA4 Appeal: 22-4489 Doc: 19-1 Filed: 01/20/2023 Pg: 116 of 184Total Pages:(116 of 2164)

J.A. 108

4. The material facts constituting probable cause that the search should be made are: ALL INFORMATION SEALED

See Attachment III.

5. The object, thing or person searched for [X] constitutes evidence of the commission of such offense [ ] is the person to be arrested for whom a warrant or process for arrest has been issued.

6. [X] I have personal knowledge of the facts set forth in this affidavit AND/OR

[ ] I was advised of the facts set forth in this affidavit, in whole or in part, by one or more other person(s). The credibility of the person(s) providing this information to me and/or the reliability of the information provided may be determined from the following facts:

Your affiant has over seven years of law enforcement experience stemming from employment as a police officer with the Chesterfield County Police Department. The undersigned is a duly appointed Task Force Officer with the Federal Bureau of Investigation (FBI). Your affiant is assigned to the Richmond FBI's Central Virginia Violent Crimes Task Force, where his duties include investigating extraterritorial offenses, commercial and bank robberies, murder, kidnappings, serial offenses, armed carjackings, and theft of government property. The undersigned has investigated numerous criminal violations and obtained multiple arrest and search warrants, culminating in the successful prosecution of their respective offenders. Your affiant is familiar with the methods violent offenders use to conduct their illegal activities, to include their communication techniques, utilization of electronic devices for planning/execution, use of additional co-conspirators, and reoccurring method of operation (MO).

The statements above are true and accurate to the best of my knowledge and belief.

Master Detective
TITLE OF APPLICANT

APPLICANT

Subscribed and sworn to before me this day.

6/14/19
DATE AND TIME

[ ] CLERK [ ] MAGISTRATE [ ] JUDGE

ALL INFORMATION SEALED

ATTACHMENT I.
PERSON, PLACE, OR THING TO BE SEARCHED:

This data is maintained on computer servers that are stored at premises controlled by Google Inc., a company that accepts service of legal process at 1600 Amphitheater Parkway, Mountain View, California 94043.

Your affiant knows that Google Inc. maintains certain records during the normal course of business and when properly served with a legal request, Google Inc. will provide Law Enforcement with the said records. Your affiant also knows that these electronic records will further support the ongoing criminal investigation. Your affiant believes that the records requested are actually or constructively possessed by a foreign corporation, Google Inc. that provides electronic communication service or remote computing service within the Commonwealth of Virginia.

Your affiant knows that section 19.2-70.3 of the Code of Virginia states that a provider of electronic communication service or remote computing service, which includes a foreign corporation that provides such services, shall disclose certain business records pertaining to their customers, excluding the contents of electronic communications and real-time location data, to an investigative or law-enforcement officer if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation. This warrant shall be properly served on the entity named above in accordance with 19.2-70.3 of the code of Virginia.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider, Google Inc. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in ATTACHMENT II.

RECEIVED & FILED
CHESTERFIELD CIRCUIT COURT
2019 JUN 14 AM 10: 31
WENDY S. HUGHES
CLERK OF COURT
BY: D.C. CLERK

ALL INFORMATION SEALED

ATTACHMENT II.
THE PLACE, PERSON OR THING TO BE SEARCHED:

The facts and circumstances outlined in this affidavit brought on by your Affiant suggest that there is probable cause to believe evidence of the commission of the crime of **Robbery**, a violation of **Virginia Code 18.2-58** and **Use of a Firearm in Commission of a Felony,** a violation of **Virginia Code 18.2-53.1**, may be found within computer servers maintained or controlled by Google, Inc. or Google Payment Corp. Such accounts are described further in ATTACHMENT II. (hereinafter "the Accounts") stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043. The following material is sought for the time period listed below:

- **Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST)**

- For each type of Google account that is associated with a device that was inside the geographical area described further in ATTACHMENT II., **during the time frame listed above,** Google will provide **"anonymized information"** regarding the Accounts that are associated with a device that was inside the described geographical area during the time frame described above. This **"anonymized information"** will include a numerical identifier for the account, the type of account, time stamped location coordinates and the data source that this information came from if available. The information initially provided by Google will not contain any further content or information identifying the user of a particular device or account.

- Law enforcement officers will review this **"anonymized information"** provided by Google, Inc. in an effort to narrow down the list of accounts associated with devices identified in the **"anonymized information."** Law enforcement officers will attempt to narrow down the list by reviewing the time stamped location coordinates for each account and comparing that against the known time and location information that is specific to this crime.

- Law enforcement officers will return a list that they have attempted to narrow down. This list will still be identified by the "**anonymized information**" described above. After this review by Law Enforcement and upon request, Google, Inc. shall produce "contextual data points with points of travel outside of the geographical area" described further in ATTACHMENT II. of this Application for Search Warrant. The time frame will be expanded for this production of "contextual data points with points of travel outside of the geographical area" for 30 minutes before AND 30 minutes after the initial search time periods. This expanded time frame will be as listed below (Google Inc. shall provide this additional information to Law Enforcement for review):

ALL INFORMATION SEALED

- **Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST) (+/- 30 Minutes) Eastern Standard Time (EST)**

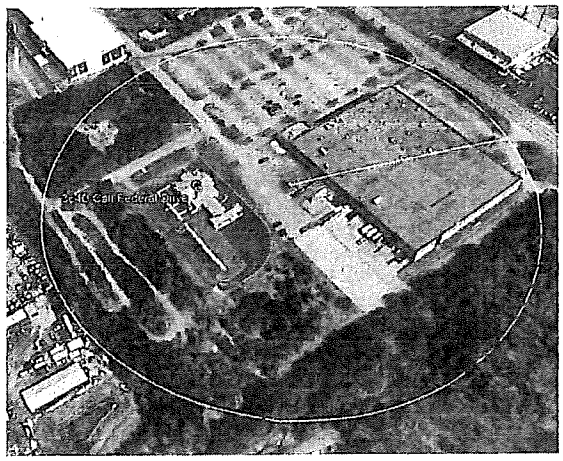
- Law Enforcement officers will review this additional information along with the **"anonymized information"** and will attempt to narrow down the list by comparing this additional information regarding travel and time against the known time and location information that is specific to this crime.

- After review and upon request by Law Enforcement, Google Inc. shall provide identifying account information/CSI for the accounts requested by Law Enforcement. This identifying account information/CSI shall include all of the following that are available: user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used to set up the account, verify the account or to receive assistance with the account, and Google Voice phone numbers associated with the account.

This search warrant applies to the Google Accounts associated with devices that were located inside the geographical regions bounded by the following latitudinal and longitudinal coordinates, dates, and times:

Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST)

Geographical Area: Radius of 150 meters around a latitude/longitude coordinate, **Latitude: 37.438420, Longitude: -77.587900.** **An area encompassing the Call Federal Credit Union and an adjacent business the UNSUB fled towards following the robbery**



RECEIVED & FILED
CHESTERFIELD CIRCUIT COURT
2019 JUN 14 AM 10:31
KEN... HUGHES
CLERK
TESTE:
CLERK

ALL INFORMATION SEALED

ATTACHMENT III.

MATERIAL FACTS CONSTITUTING PROBABLE CAUSE:

The Affiant swears to the following facts to establish probable cause for the issuance of a search warrant:

On 05/20/2019 at approximately 1650 hours, an unknown subject (UNSUB) entered the Call Federal Credit Union, [redacted] Call Federal Drive, Chesterfield, VA 23235. After entering the bank, the UNSUB approached a teller line and presented a demand note stating the following:

"I've been watching you for sometime now. I got your family as hostage and I know where you live, If you or your coworker alert the cops or anyone your family and you are going to be hurt. I got my boys on the lookout out side. The first cop car they see am going start hurting everyone in sight, hand over all the cash, I need at least 100k and nobody will get hurt and your family will be set free. Think smartly everyone safety is depending and you and your coworkers action so I hope they don't try nothing stupid."

After reading the note, the victim-teller advised she did not have access to that amount of money; subsequently, the UNSUB produced a silver and black firearm from his waste and began forcing the customers and employees to the center of the room. After forcing several patrons to the floor at gunpoint, the UNSUB moved the manager and other parties present to the back of the business where the vault was located. The UNSUB forced the manager to open the vault and place $195,000.00 of United States currency into a bag he brought with him. After acquiring said funds, the UNSUB fled the area on foot towards an adjacent business, west of the bank.

Upon investigative response, law enforcement officials reviewed the bank's surveillance video prior to the robbery and noted the UNSUB had a cell phone in his right hand and appeared to be speaking with someone on the device. Subsequently, your affiant finds it necessary and prudent to request that Google provide Geo Fencing data in order to assist with the investigation. In the undersigned's training and experience, when people act in concert with one another to commit a crime, they frequently utilize cellular telephones and other such electronic devices, to communicate with each other through WiFi, Bluetooth, GPS, voice calls, text messages, social media accounts, applications, emails, and/or cell towers in the area of the victim-business, located at [redacted] Call Federal Drive, Chesterfield, Virginia 23235. Furthermore, the requested data/information would have been captured by Google during the requested time.

This applicant knows a cellular telephone or mobile telephone is a handheld wireless device primarily used for voice, text, and data communication through radio signals.

ALL INFORMATION SEALED

Cellular telephones send signals through networks of transmitter/receivers called "cells" or "cell sites," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") or other technology for determining a more precise location of the device.

This applicant also knows that Google is a company, which, among other things, provides electronic communication services to subscribers, including email services. Google allows subscribers to obtain email accounts at the domain name gmail.com and/or google.com. Subscribers obtain an account by registering with Google. A subscriber using the Provider's services can access his or her email account from any computer/device connected to the Internet.

This applicant knows that Google has also developed a proprietary operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

Based on this applicant's training and experience, this applicant knows that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled. The company uses this information for location-based advertising and location-based search results and stored such data in perpetuity unless it is manually deleted by the user. This location information is derived from GPS data, cell site/cell tower information, Bluetooth connections, and Wi-Fi access points.

This applicant knows that location data can assist investigators in forming a fuller geospatial understanding and timeline related to a specific criminal investigation; and may tend to identify potential witnesses and/or suspects. Such information can also aid investigators in possibly inculpating or exculpating persons of interest.

Additionally, location information can be digitally integrated into image, video, or other computer files associated with a Google account and can indicate the geographic location of the account's user at a particular date and time (e.g., digital cameras, including on cellular telephones, frequently store GPS coordinates indicating where a photo was taken in the "metadata" of an image file).

Your affiant knows that in the September 2013 Pew Research Center study, it was determined that 91% of American adults own a cellular phone with 56% being smartphones. Pew Research Center is located at 1615 L St. NW, Suite 800 Washington, DC 20036 and conduct public opinion polling, demographic research, content analysis and other data-driven social science research. Because of this, your Affiant believes that there is probable cause to believe that the offender(s) in the robbery would have had a mobile device on their person or within close proximity to them.

USCA4 Appeal: 22-4489 Doc: 19-1 Filed: 01/20/2023 Pg: 122 of 184Total Pages:(122 of 2164)

ALL INFORMATION SEALED

SEARCH WARRANT

Commonwealth of Virginia VA. CODE §§ 19.2-56, 19.2-57

TO ANY AUTHORIZED OFFICER:

You are hereby commanded in the name of the Commonwealth to forthwith search the following place, person or thing either in day or night

Google, LLC. which is headquartered at 1600 Google Amphitheater Parkway, Mountain View, California 94043 - Probable cause that the records are possessed by a foreign corporation that provides electronic communication service orremote computing service within Virginia.

for the following property, objects and/or persons:
See Attached

You are further commanded to seize said property, persons, and/or objects if they be found and to produce before the Chesterfield Circuit Court an inventory of all property, persons, and/or objects seized.

This SEARCH WARRANT is issued in relation to [X] an offense substantially described as follows:
[ ] a person to be arrested for whom a warrant or process for arrest has been issued identified as follows:
Code of Virginia 18.2-58 Robbery
Code of Virginia 18.2-53.1 Use of a Firearm in the Commission of a Felony

I, the undersigned, have found probable cause to believe that the property or person constitutes evidence of the crime identified herein or tends to show that the person(s) named or described herein has committed or is committing a crime, or that the person to be arrested for whom a warrant or process for arrest has been issued is located at the place to be searched, and further that the search should be made, based on the statements in the attached affidavit sworn to by

Hylton, J.P. CPD[redacted]
NAME OF AFFIANT

06/14/2019 10:06 AM
DATE AND TIME

David Bishop
[ ] CLERK [X] MAGISTRATE [ ] JUDGE

FORM DC-339 (MASTER, PAGE ONE OF TWO) 07/17

FILE NO. 7446

SEARCH WARRANT

COMMONWEALTH OF VIRGINIA

v./*In re*

Google LLC

Return to Circuit Court

ORIGINAL

SWN: 041CM1900017880

J.A. 114

USCA4 Appeal: 22-4489 Doc: 19-1 Filed: 01/20/2023 Pg: 123 of 184Total Pages:(123 of 2164)

J.A. 115

ALL INFORMATION SEALED

SEARCH INVENTORY AND RETURN

The following items, and no others, were seized under authority of this WARRANT:

1. Data
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

RECEIVED & FILED
CHESTERFIELD CIRCUIT COURT
WENDY S. HUGHES, CLERK
JUN 19 2019
TESTE:
☐ CLERK ☐ DEPUTY CLERK

The statement above is true and accurate to the best of my knowledge and belief.

6/19/2019
DATE

EXECUTING OFFICER

Subscribed and sworn before me this day

6.19.19
DATE

[ ] CLERK [ ] MAGISTRATE [ ] JUDGE

FOR NOTARY PUBLIC'S USE ONLY:

State of ..... [ ] City [ ] County of .....

Acknowledged, subscribed and sworn to before me this ..... day of ....., 20 .....

NOTARY REGISTRATION NUMBER

NOTARY PUBLIC
(My commission expires: .....)

FORM DC-339 (MASTER, PAGE TWO OF TWO) 01/09

EXECUTION

Executed by searching the within described place, person or thing.

6/14/2019 at 1030 Hrs
DATE AND TIME EXECUTED

Hylton
EXECUTING OFFICER

Certified to Chesterfield County
Circuit Court on 6/19/2019
DATE

EXECUTING OFFICER

Received [ ] in person [ ] by certified mail
[ ] by electronically transmitted facsimile

on 6.19.19
DATE

by:
CLERK OF CIRCUIT COURT

ALL INFORMATION SEALED

ATTACHMENT I.
THE PLACE, PERSON OR THING TO BE SEARCHED:

The facts and circumstances outlined in this affidavit brought on by your Affiant suggest that there is probable cause to believe evidence of the commission of the crime of **Robbery**, a violation of **Virginia Code 18.2-58** and **Use of a Firearm in Commission of a Felony,** a violation of **Virginia Code 18.2-53.1**, may be found within computer servers maintained or controlled by Google, Inc. or Google Payment Corp. Such accounts are described further in ATTACHMENT II. (hereinafter "the Accounts") stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043. The following material is sought for the time period listed below:

- **Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST)**

- For each type of Google account that is associated with a device that was inside the geographical area described further in ATTACHMENT II., **during the time frame listed above,** Google will provide **"anonymized information"** regarding the Accounts that are associated with a device that was inside the described geographical area during the time frame described above. This **"anonymized information"** will include a numerical identifier for the account, the type of account, time stamped location coordinates and the data source that this information came from if available. The information initially provided by Google will not contain any further content or information identifying the user of a particular device or account.

- Law enforcement officers will review this **"anonymized information"** provided by Google, Inc. in an effort to narrow down the list of accounts associated with devices identified in the **"anonymized information."** Law enforcement officers will attempt to narrow down the list by reviewing the time stamped location coordinates for each account and comparing that against the known time and location information that is specific to this crime.

- Law enforcement officers will return a list that they have attempted to narrow down. This list will still be identified by the "**anonymized information**" described above. After this review by Law Enforcement and upon request, Google, Inc. shall produce "contextual data points with points of travel outside of the geographical area" described further in ATTACHMENT II. of this Application for Search Warrant. The time frame will be expanded for this production of "contextual data points with points of travel outside of the geographical area" for 30 minutes before AND 30 minutes after the initial search time periods. This expanded time frame will be as listed below (Google Inc. shall provide this additional information to Law Enforcement for review):

ALL INFORMATION SEALED

- **Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST) (+/- 30 Minutes) Eastern Standard Time (EST)**

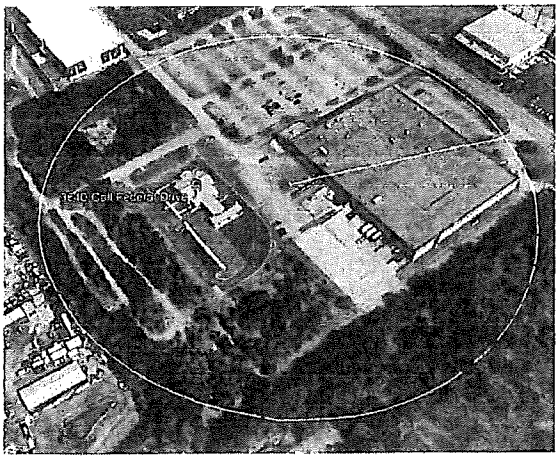
- Law Enforcement officers will review this additional information along with the **"anonymized information"** and will attempt to narrow down the list by comparing this additional information regarding travel and time against the known time and location information that is specific to this crime.

- After review and upon request by Law Enforcement, Google Inc. shall provide identifying account information/CSI for the accounts requested by Law Enforcement. This identifying account information/CSI shall include all of the following that are available: user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used to set up the account, verify the account or to receive assistance with the account, and Google Voice phone numbers associated with the account.

This search warrant applies to the Google Accounts associated with devices that were located inside the geographical regions bounded by the following latitudinal and longitudinal coordinates, dates, and times:

Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST)

Geographical Area: Radius of 150 meters around a latitude/longitude coordinate, **Latitude: 37.438420, Longitude: -77.587900.** **An area encompassing the Call Federal Credit Union and an adjacent business the UNSUB fled towards following the robbery**



RECEIVED & FILED
CHESTERFIELD CIRCUIT COURT
2019 JUN 14 AM 10:30
WENDY S. HUGHES
CLERK OF COURT
DATE:
D. CLERK

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA v. OKELLO T. CHATRIE, *Defendant*.	Case No. 3:19-cr-00130-MHL

BRIEF OF AMICUS CURIAE GOOGLE LLC IN SUPPORT OF NEITHER PARTY CONCERNING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE FROM A "GEOFENCE" GENERAL WARRANT (ECF NO. 29)

DISCLOSURE STATEMENT

Pursuant to Local Criminal Rule 12.4, Google hereby discloses that it is an indirect subsidiary of Alphabet Inc., a publicly traded company. No publicly traded company holds more than 10% of Alphabet Inc.'s stock.

TABLE OF CONTENTS

Page

DISCLOSURE STATEMENT i

TABLE OF AUTHORITIES iii

INTEREST OF AMICUS CURIAE 1

INTRODUCTION AND SUMMARY OF ARGUMENT 2

ARGUMENT 5

I. GOOGLE "LOCATION HISTORY" INFORMATION DIFFERS SIGNIFICANTLY FROM CELL SITE LOCATION INFORMATION AND OTHER TYPES OF LOCATION DATA COURTS HAVE CONSIDERED IN OTHER FOURTH AMENDMENT CASES 5

A. Google "Location History" Is Not A Business Record, But A Journal Of A User's Location And Travels That Is Created, Edited, And Stored By And For The Benefit Of Google Users Who Have Opted Into The Service 6

B. Google LH Data Can Reflect A User's Movements More Precisely Than CSLI And Other Types Of Data 10

C. Collecting And Producing Google LH Information To Law Enforcement In Response To A Geofence Request Requires A Uniquely Broad Search Of All Google Users' Timelines 11

II. THE STORED COMMUNICATIONS ACT REQUIRES THE GOVERNMENT TO OBTAIN A WARRANT TO COMPEL PRODUCTION OF "LOCATION HISTORY" INFORMATION 14

III. ABSENT AN APPLICABLE EXCEPTION, THE FOURTH AMENDMENT REQUIRES THE GOVERNMENT TO OBTAIN A WARRANT TO COMPEL PRODUCTION OF "LOCATION HISTORY" INFORMATION 18

CONCLUSION 24

TABLE OF AUTHORITIES

Page(s)

CASES

Camara v. Municipal Court,
387 U.S. 523 (1967).....19

Carpenter v. United States,
138 S. Ct. 2206 (2018)..... *passim*

In re Application of the United States of America for a Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210 (D. Or. 2009).....15

In re Certified Question of Law,
858 F.3d 591 (Foreign Int. Surv. Ct. Rev. 2016).....18

In re Google Inc. Cookie Placement Consumer Privacy Litigation,
806 F.3d 125 (3d Cir. 2015).....17, 18

In re Grand Jury, John Doe No. G.J.2005-2,
478 F.3d 581 (4th Cir. 2007) 2

Katz v. United States,
389 U.S. 347 (1967).....19

Riley v. California,
573 U.S. 373 (2014).....20, 23

Smith v. Maryland,
442 U.S. 735 (1979).....21, 22, 23

United States v. Aigbekaen,
943 F.3d 713 (4th Cir. 2019) 20

United States v. Beverly,
943 F.3d 225 (5th Cir. 2019) 10

United States v. Finley,
477 F.3d 250 (5th Cir. 2007) 22

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) (en banc) 15, 17

United States v. Jones,
565 U.S. 400 (2012).....20, 22

United States v. Miller,
425 U.S. 435 (1976).....21, 22, 23

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 15, 18, 22

STATUTES AND RULES

18 U.S.C.
§ 2510.....16
§ 2701.....2, 11
§ 2703.....2, 4, 15, 16, 18

Fed. R. Crim. P.
17.....2
41.....4

OTHER AUTHORITIES

Google, *Choose Which Apps Use Your Android Phone's Location*,
https://support.google.com/android/answer/6179507 (visited Dec. 20, 2019) 7

Google, *Find And Improve Your Location's Accuracy*,
https://support.google.com/maps/answer/2839911 (visited Dec. 20, 2019).....10

Google, *Manage Your Android Device's Location Settings*,
https://support.google.com/accounts/answer/3467281 (visited Dec. 20, 2019) 7

Google, *Manage Your Location History*,
https://support.google.com/accounts/answer/3118687 (visited Dec. 20, 2019) 7, 8

H.R. Rep. No. 114-528 (2016).....15

Kerr, Orin, Volokh Conspiracy, Wash. Post, *Websurfing and the Wiretap Act*,
(June 4, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/ 17

Valentino-DeVries, Jennifer, N.Y. Times, *Tracking Phones, Google Is a Dragnet for the Police* (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html 13

Webster, Tony, Minnesota Public Radio, *How Did The Police Know You Were Near A Crime Scene? Google Told Them* (Feb. 7, 2019),
https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants 13

INTEREST OF AMICUS CURIAE[1]

Google LLC ("Google") is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of products and services, including the Android and Chrome operating systems, as well as Google Search, Maps, Drive, and Gmail. Among those products and services is Google Location History ("LH"), which allows individual users who have chosen to use the LH service to create, edit, and save records of their whereabouts over time—akin to journal entries of journeys taken and places visited. The warrant at issue in this motion compelled Google to produce data associated with Chatrie and other Google users—specifically, data from Google's LH service.

When using LH and other services, Google users routinely entrust private, personal data, including location-related information, to Google for processing and storage. Google recognizes and respects the privacy of this information and is transparent with users about when and how their information is stored. For example, Google's Privacy Policy informs users about their data, how to keep it safe, and how to take control. And Google regularly publishes transparency reports that reflect the volume of requests for disclosure of user data that Google receives from government entities.

Google respectfully submits this amicus brief in support of neither party to provide contextual information to the Court about the data at issue in Defendant Chatrie's motion to suppress evidence obtained from a so-called "geofence" warrant. *See* Mot. to Suppress Evidence

[1] The undersigned certifies that no party or party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was used to fund the preparation or submission of this brief; and no persons other than amicus curiae or its counsel contributed money that was intended to fund the preparation or submission of this brief.

Obtained From a "Geofence" General Warrant (ECF No. 29) ("Mot."); Govt. Response in Opp. to Def.'s Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (ECF No. 41) ("Opp."). That warrant compelled Google to produce users' LH information, so an understanding of that information—including what it is, how users can create and save it, and what Google must do to comply with a warrant to produce it—is needed to resolve the parties' legal arguments on the motion to suppress. While the parties' briefs reveal some uncertainty about certain aspects of LH that are relevant to the questions presented by the motion, Google is well situated to explain the nature of the data and the steps Google takes in response to geofence warrants like the one at issue here. Moreover, because law-enforcement requests for this type of data have become increasingly common in recent years, Google also has a significant interest in the constitutional and statutory requirements and limitations that govern law enforcement efforts to obtain LH information. While Google takes no position on the validity of the warrant at issue in this case or whether the evidence it yielded should be suppressed, it respectfully urges the Court to take into account the full factual context surrounding the warrant and hold that both the Stored Communications Act, 18 U.S.C. § 2703, and the Fourth Amendment require the government to obtain a warrant supported by probable cause to obtain LH information stored by Google users.[2]

INTRODUCTION AND SUMMARY OF ARGUMENT

Pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, law enforcement can and frequently does obtain legal process compelling Google to disclose the contents or

[2] By submitting this brief as amicus curiae, Google does not become a party to the case and does not waive any objections it might have to any efforts by the parties to obtain discovery or testimony from Google. *See, e.g.*, Fed. R. Crim. P. 17(c)(2); *In re Grand Jury, John Doe No. G.J.2005-2*, 478 F.3d 581, 585 (4th Cir. 2007) ("Courts have recognized various ways in which a subpoena may be unreasonable or oppressive under Rule 17(c).").

records of particular users' stored electronic communications, including data that reveals those persons' locations and movements at particular times of interest. Such requests typically seek to compel disclosure of information pertaining to specifically identified persons of interest in a criminal investigation.

This case, in contrast, concerns a novel but rapidly growing technique in which law enforcement seeks to require to search across LH data, using legal requests sometimes called "geofence" requests. Rather than seeking information relating to a known suspect or person of interest, these requests broadly seek to identify all Google LH users whose LH data suggests that they were in a given area in a given timeframe—even though law enforcement has no particularized basis to suspect that all of those users played a role in, or possess any information relevant to, the crime being investigated. State and federal law-enforcement authorities have made increasing use of this technique in recent months and years. Year over year, Google has observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and to date, the rate has increased over 500% from 2018 to 2019.

As set forth below, the LH information at issue in geofence requests such as the one in this case differs in significant respects from the cell site location information ("CSLI") at issue in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and other types of data that courts have considered in Fourth Amendment cases. For example, rather than a record created and stored by Google as an automatic result of using a Google service, Google LH information is created, edited, and stored by and for the benefit of Google users who opt into the service and choose to communicate their location information to Google for storage and processing. Moreover, LH information can often reveal a user's location and movements with a much higher degree of precision than CSLI and other types of data. And rather than targeting the electronic

communications of only a specific user or users of interest, the steps Google must take to respond to a geofence request entail the government's broad and intrusive search across Google users' LH information to determine which users' devices may have been present in the area of interest within the requested timeframe.

Given the characteristics of geofence requests, the law requires the government to obtain a warrant to require Google to search LH information. First, although the parties have not addressed the statutory context, the Stored Communications Act ("SCA")—quite apart from the Constitution—requires the government to obtain a search warrant because a geofence request seeks the "contents" of Google users' electronic communications within the meaning of the SCA. *See* 18 U.S.C. § 2703(a), (b). Therefore, regardless of whether a geofence request amounts to a "search" for Fourth Amendment purposes, the government must obtain a warrant from a neutral magistrate that satisfies the requirements of probable cause and particularity. *See id.* (incorporating requirements of Fed. R. Crim. P. 41).

In any event, it is also clear that a geofence request constitutes a "search" within the meaning of the Fourth Amendment and that, absent an applicable exception, the Constitution independently requires the government to obtain a warrant to obtain LH information. Users have a reasonable expectation of privacy in their LH information, which the government can use to retrospectively reconstruct a person's movements in granular detail. Under *Carpenter*, the "third-party doctrine" does not defeat that reasonable expectation of privacy merely because users choose to store and process the information on Google' servers.

Whether under the SCA or under the Fourth Amendment—and absent an applicable exception—the government is therefore obligated to obtain a warrant to search LH information. That requirement is entirely appropriate in light of the sensitivity of LH information, the intimate

details it can reveal about a user's life, and the breadth of the government's intrusion on users' private LH information that occurs whenever a geofence search is executed. Google's users expect their LH information to be kept private, and the Court should ensure that it receives the greatest available protection. Google takes no position on Defendant Chatrie's arguments that the warrant at issue here failed to satisfy the requirements of probable cause and particularity or, if so, whether suppression is the appropriate remedy. But the Court should hold—taking account of the full factual context—that a warrant is indeed required.

ARGUMENT

I. GOOGLE "LOCATION HISTORY" INFORMATION DIFFERS SIGNIFICANTLY FROM CELL SITE LOCATION INFORMATION AND OTHER TYPES OF LOCATION DATA COURTS HAVE CONSIDERED IN OTHER FOURTH AMENDMENT CASES

While many of Google's products and services can be used without a Google account, millions of people choose to create Google accounts and log into them from their mobile devices or while using Google applications to take full advantage of account-specific products such as Gmail and to obtain a more personalized experience on applications such as Maps and Search. Holders of Google accounts can control various account-level and service-level settings and preferences. "Location History" (or "LH") is an optional account-level Google service. It does not function automatically for Google users. But when users opt into LH on their Google accounts, it allows those users to keep track of locations they have visited while in possession of their mobile devices.

In the briefing, the parties analogize the LH information at issue in this case to CSLI, "tower dumps," GPS data, and other types of location information that courts have considered in other cases. Mot. 2, 14; Opp. 7-8, 11-12, 18. In fact, while Google LH information bears some similarities to those types of data in some respects, it differs in important ways that are highly

relevant to the question whether a warrant is required. In determining the legal framework governing law enforcement requests for Google LH information, the court should therefore proceed with an understanding of the nature and precision of that information, how it is recorded and stored, how users control it, and how it is collected in response to legal process.

A. Google "Location History" Is Not A Business Record, But A Journal Of A User's Location And Travels That Is Created, Edited, And Stored By And For The Benefit Of Google Users Who Have Opted Into The Service

Google "Location History" information is essentially a history or journal that Google users can choose to create, edit, and store to record their movements and travels. Google's users activate and use LH for many reasons. By enabling and using LH, a Google user can keep a virtual journal of her whereabouts over a period of time. For most Google users, this journal is captured in the "Timeline" feature of the Google Maps app. *See* Fig. 1. The Timeline feature allows the user to visualize where she has traveled with her phone and when over a given period—in essence, a journal. The Timeline might reflect, for instance, that the user left her home on Elm Street in the morning and walked to the bus stop, took the bus to her office on Main Street, walked to a nearby coffee shop and back to the office in the afternoon, and then went to a nearby restaurant in the evening before returning home by car.

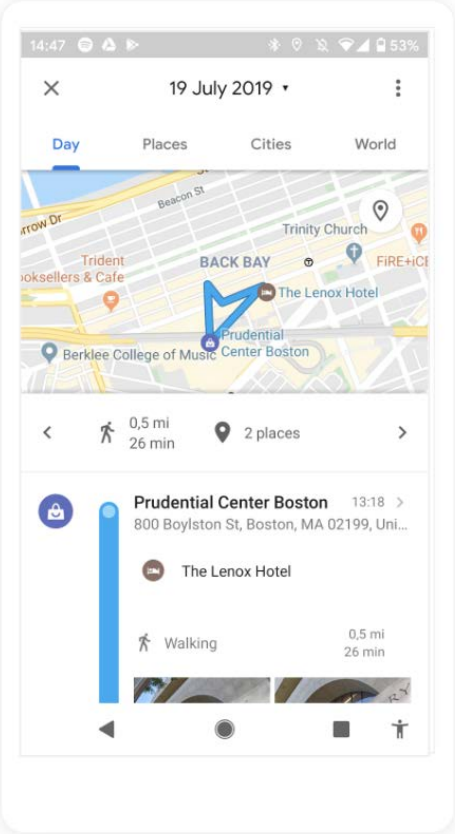


Figure 1. Sample Google Timeline.

By using Google LH, the user can access other benefits on her Google device or applications as well. For example, she can obtain personalized maps or recommendations based

on places she has visited, get help finding her phone, and receive real-time traffic updates about her commute.[3]

For Google LH to function and save information about a user's location, the user must take several steps—some tied to her mobile device, some tied to her Google account. First, the user must ensure that the device-location setting on her mobile device is turned on. When the device-location setting is activated, the mobile device automatically detects its own location, which the device ascertains based on GPS and Bluetooth signals, Wi-Fi connections, and cellular networks.[4] Second, the user must configure her mobile device to share location information with applications capable of using that information. Not all mobile applications can use location information, and those that can, such as Google Maps, will do so only if the user configures her device to allow the app to use the mobile device's location information.

Critically, merely taking the steps described above that are tied to the mobile device does not on its own generate a saved LH record of a Google user's locations. Google does not save information about where a particular mobile device has been to a user's account—even when the device-location feature is turned on and applications on the device are using location data—unless the user has also taken additional specific steps tied to her Google account. Specifically, the user must opt into LH in her account settings and enable "Location Reporting"—a subsetting

[3] *See* Google, *Manage Your Location History*, https://support.google.com/accounts/answer/3118687 (visited Dec. 20, 2019).

[4] Android users can tailor their devices' location-reporting settings, controlling which sources of information (*e.g.*, GPS, cellular, or Wi-Fi) are detectable from the device, and which applications can access location data. *See, e.g.*, Google, *Manage Your Android Device's Location Settings*, https://support.google.com/accounts/answer/3467281 (visited Dec. 20, 2019); Google, *Choose Which Apps Use Your Android Phone's Location*, https://support.google.com/android/answer/6179507 (visited Dec. 20, 2019).

within LH—for the particular device.[5] And to actually record and save LH data, the user must then sign into her Google account on her device and travel with that device. In sum, LH functions and saves a record of the user's travels only when the user opts into LH as a setting on her Google account, enables the "Location Reporting" feature for at least one mobile device, enables the device-location setting on that mobile device, permits that device to share location data with Google, powers on and signs into her Google account on that device, and then travels with it.

When a user takes those steps, the resulting data is communicated to Google for processing and storage on Google's cloud-based servers, and to enable Google to make it available to the user in various ways. But it is the user who controls the LH information. The user can review, edit, or delete her Timeline and LH information from Google's servers at will. For example, the user could decide to keep LH information only for dates when she was traveling abroad and manually delete the rest; she could delete all Timeline entries except those associated with visits to memorable restaurants; she could instruct Google to automatically delete all LH information after a set period (say, every three months); or she could keep all LH information for future reference.

The user thus controls her Google LH data—unlike, for instance, the CSLI at issue in *Carpenter* or cellular data obtained via a "tower dump." As the Supreme Court explained in *Carpenter*, CSLI consists of time-stamped records that are automatically generated by and for the wireless carrier whenever a mobile device connects to a cell site (*i.e.*, the physical radio

[5] A Google account may be associated with multiple devices. The "Location Reporting" feature within LH allows users to select specific devices on which to enable LH. *See* Google, *Manage Your Location History*, https://support.google.com/accounts/answer/3118687 (visited Dec. 20, 2019).

antennas that make up the cellular network). 138 S. Ct. at 2211-2212. Wireless carriers collect and maintain CSLI records "for their own business purposes," such as identifying weak spots in the network or determining when to apply roaming charges. *Id.* at 2212. When law enforcement seeks access to CSLI, it is thus asking the wireless carrier to produce its own business records showing when a particular device connected to a cell site within a particular period of time. A request for a "tower dump" likewise seeks the wireless carrier's own business records—in that case, identifying every phone that connected to a particular cell site (or "tower") in a particular period.

Mobile device users cannot opt out of the collection of CSLI or similar records, nor can they retrieve, edit, or delete CSLI data. Google LH information, by contrast, is stored with Google primarily for the user's own use and benefit—just as a user may choose to store her emails on Google's Gmail service and her documents on Google Drive. Google LH information is controlled by the user, and Google stores that information in accordance with the user's decisions (*e.g.*, to opt in or out, or to save, edit, or delete the information), including to enhance the user's experience when using other Google products and services. *Supra* pp. 6-8.

Defendant thus errs in asserting that "[i]ndividuals do not voluntarily share their location information with Google," Mot. 10, and that the acquisition of user location records by Google is "automatic and inescapable," Reply 6. As discussed, Google does not save LH information unless the user opts into the LH service in her account settings (and logs into her Google account while using a properly configured mobile device), and the user can choose at any time to delete some or all of her saved LH information or to disable the LH service completely. And LH information was the only location information produced to the government in response to this geofence warrant.

B. Google LH Can Reflect A User's Location and Movements More Precisely Than CSLI And Other Types Of Data

Google LH information can be considerably more precise than other kinds of location data, including the CSLI considered in *Carpenter*. That is because, as a technological matter, a mobile device's location-reporting feature can use multiple inputs in estimating the device's location. Those inputs include not only information related to the locations of nearby cell sites, but also GPS signals (*i.e.*, radio waves detected by a receiver in the mobile device from orbiting geolocation satellites) or signals from nearby Wi-Fi networks or Bluetooth devices. Combined, these inputs (when the user enables them) can be capable of estimating a device's location to a high degree of precision. For example, when a strong GPS signal is available, a device's location can be estimated within approximately twenty meters.[6]

CSLI, by contrast, shows a less-detailed picture of a mobile device's movements. Although its precision has increased as wireless carriers have introduced more and more cell towers that cover smaller and smaller areas, it typically reflects location on the order of dozens to hundreds of city blocks in urban areas rather than a matter of meters, and up to forty times more imprecise in rural areas. *See Carpenter*, 138 S. Ct. at 2225 (Kennedy, J. dissenting); *see also United States v. Beverly*, 943 F.3d 225, 230 n.2 (5th Cir. 2019) ("CSLI should not be confused with GPS data, which is far more precise location information derived by triangulation between the phone and various satellites.").[7]

---

[6] *See* Google, *Find And Improve Your Location's Accuracy*, https://support.google.com/maps/answer/2839911 (visited Dec. 20, 2019).

[7] No estimate is perfect, and the estimated locations reflected in Google LH are no exception. Like any probabilistic estimate based on multiple inputs, the estimated locations reflected in Google LH have a margin of error, so a user's actual location will not always align with any one estimated location data point in LH. In that respect, LH differs from CSLI, which is not an estimate at all, but simply a historical fact: that a device connected to a given cell tower

C. Collecting And Producing Google LH Information To Law Enforcement In Response To A Geofence Request Requires A Uniquely Broad Search Of All Google Users' Timelines

The Stored Communications Act ("SCA") governs how service providers such as Google handle the contents and records of their users' stored electronic communications, including Google LH. In general, the SCA prohibits unauthorized access to those stored communications, restricts the service provider's ability to disclose them to the government, and delineates the procedures law enforcement must follow—and the substantive standards it must meet—to compel a service provider to produce them. *See* 18 U.S.C. §§ 2701 *et seq.*

Typically, U.S. law-enforcement authorities use legal process (whether in the form of a search warrant, court order, or subpoena) to compel Google to disclose content or records of electronic communications associated with specifically identified Google users or accounts. For example, the government might obtain a warrant for the contents of emails associated with a particular Gmail account. Google often receives warrants for LH information that take the same form—*i.e.*, demands for a specifically identified Google user's LH information from a specifically identified time range. When producing data in response to such a demand, Google must search for and retrieve only the responsive data that is associated with the particular users or accounts identified in the warrant.

So-called "geofence" requests operate quite differently. Geofence requests represent a new and increasingly common form of legal process that is not tied to any known person, user, or account. Instead, law enforcement uses geofence requests in an attempt to identify all Google users who might have stored LH data in their accounts suggesting that they were near a given

---

during a given time period. An LH user's Timeline, however, combines and contextualizes numerous individual location data points, so that the resulting picture of the user's location and movements is sufficiently precise and reliable for the purposes for which it was designed.

area in a given timeframe—and to do so at a level of precision not available through CSLI or similar data.

Such requests typically identify a geographic area surrounding a point of interest. That point of interest is typically a suspected crime scene. As Defendant observes (at Mot. 12-13), however, the geographic area can also include private homes, government buildings, places of worship, and other sensitive locations. A geofence request seeks to compel Google to produce LH information for all Google users whose LH records indicate that they may have been present in the defined area within a certain window of time, which might span a few minutes or a few hours. (In practice, although the legal requests do not necessarily reflect this limitation, such requests can cover only Google users who had LH enabled and were using it at the time in question.)

Many of the earliest "geofence" legal requests attempted to mimic "tower dump" requests, seeking LH data that would identify all Google users who were in a geographical area in a given time frame. In light of the significant differences between CSLI and Google LH data described above, however, Google developed a multi-step anonymization and narrowing protocol to ensure privacy protections for its users. That protocol typically entails a three-step process:

First, law enforcement obtains legal process compelling Google to disclose an anonymized list of all Google user accounts for which there is saved LH information indicating that their mobile devices were present in a defined geographic area during a defined timeframe. Google, however, has no way to know ex ante which users may have LH data indicating their potential presence in particular areas at particular times. In order to comply with the first step of the geofence protocol, therefore, Google must search across all LH journal entries to identify

users with potentially responsive LH data, and then run a computation against every set of coordinates to determine which LH records match the time and space parameters in the warrant.

After Google has completed that search, it assembles the LH information that is responsive to the request without any account-identifying information. This anonymized "production version" of the data includes an anonymized device number, the latitude/longitude coordinates and timestamp of the reported location information, the map's display radius,[8] and the source of the reported location information (that is, whether the location was generated via Wi-Fi, GPS, or a cell tower). The volume of data produced at this stage depends on the size and nature of the geographic area and length of time covered by the geofence request, which vary considerably from one request to another.[9]

Second, the government reviews the anonymized production version to identify the anonymized device numbers of interest. If additional anonymized location information for a specific device is necessary to eliminate false positives or otherwise determine whether that device is actually relevant to the investigation, law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request. Here, for example, the government requested a second round of anonymized LH information showing where certain users moved during an extended period of time 30 minutes

[8] Each set of coordinates saved to a user's LH includes a value, measured in meters, that reflects Google's confidence in the reported coordinates. A value of 100 meters, for example, reflects Google's estimation that the user is likely located within a 100-meter radius of the reported coordinates.

[9] *See, e.g.*, Jennifer Valentino-DeVries, N.Y. Times, *Tracking Phones, Google Is a Dragnet for the Police* (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html (discussing examples); Tony Webster, Minnesota Public Radio, *How Did The Police Know You Were Near A Crime Scene? Google Told Them* (Feb. 7, 2019), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants (same).

before and 30 minutes after the original timeframe. This additional contextual LH information can assist law enforcement in eliminating devices that were not in the target location for enough time to be of interest, were moving through the target location in a manner inconsistent with other evidence, or otherwise are not relevant to the investigation. The government then reviews users' movements, as reflected in the anonymized data, and selects the anonymized device numbers for which it will require Google to produce identifying user account information.

Third, the government can compel Google to provide account-identifying information for the anonymized device numbers that it determines are relevant to the investigation. Typically, the legal request requires Google to provide account subscriber information such as the Gmail address associated with the account and the first and last name entered by the user on the account.

The steps necessary to respond to a geofence request are thus quite different from and far more intrusive than responses to requests for CSLI or "tower dumps." To produce a particular user's CSLI, a cellular provider must search its records only for information concerning that particular user's mobile device. A tower dump is similarly limited: It requires a provider to produce only records of the mobile devices that connected to a particular cell tower at a particular time. But because Google LH information on a user's account is distinct from a mobile device's location-reporting feature, Google has no way to identify which of its users were present in the area of interest without searching the LH information stored by every Google user who has chosen to store that information with Google.

II. THE STORED COMMUNICATIONS ACT REQUIRES THE GOVERNMENT TO OBTAIN A WARRANT TO COMPEL PRODUCTION OF "LOCATION HISTORY" INFORMATION

Although the parties' briefing has focused on the Fourth Amendment, the Court's resolution of the important questions presented here should reflect the entire legal landscape.

Google's storage and disclosure of user data, including LH information, is subject to the SCA, which governs law-enforcement efforts to compel service providers such as Google to disclose data relating to a user's stored electronic communications. *See* 18 U.S.C. § 2703. The SCA generally requires the government to obtain a warrant supported by probable cause to require a provider to disclose the "contents" of electronic communications (such as the contents of an email). *Id.* § 2703(a), (b)(1)(A); *United States v. Graham*, 824 F.3d 421, 437 (4th Cir. 2016) (en banc), *overruled on other grounds*, 138 S. Ct. 2206.[10] By contrast, if the government uses legal process requiring a less demanding showing than probable cause—such as a court order or subpoena—it can generally only compel the production by a provider of basic subscriber information (using a subpoena) and other "records" of electronic communications, such as data indicating when an email was sent or to whom, but without the content of the email (using a court order). *See* 18 U.S.C. § 2703(c), (d).

[10] The SCA draws a distinction between government access to the contents of electronic communications in "electronic storage in an electronic communications system for one hundred and eighty days or less"—for which a warrant is invariably required—and access to the contents of electronic communications in "electronic storage in an electronic communications system for more than one hundred and eighty days" or contents of electronic communications "in a remote computing service," for which a warrant is required unless the government complies with certain notice procedures. 18 U.S.C. § 2703(a), (b). That distinction, which reflected the technical landscape prevailing at the time of the SCA's enactment in 1986, has largely fallen into disuse. The statutory provisions purporting to allow warrantless access to "contents" of communications under certain conditions without a warrant have been held unconstitutional, *see United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), and the Department of Justice has followed that holding as a matter of policy since 2013 by always using warrants to obtain stored content, *see* H.R. Rep. No. 114-528, at 9 (2016). In any event, Google acts as a provider of both an "electronic communication service" and a "remote computing service" in regard to LH information, and the information sought in this case was in storage for less than 180 days at the time of the warrant, rendering these statutory distinctions irrelevant in this case. *See In re Application of the United States of America for a Search Warrant for Contents of Elec. Mail and for an Order Directing a Provider of Elec. Comm'cn Servs. to not Disclose the Existence of the Search Warrant*, 665 F. Supp. 2d 1210, 1213 (D. Or. 2009) ("Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time … , rather than to define the service provider itself.").

Google LH information is subject to the SCA's warrant requirement because that information qualifies as "contents" of "electronic communications." The SCA defines an "electronic communication" as a "transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part" by an electronic system. 18 U.S.C. § 2510(12). And it defines the "contents" of such a communication as "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8). A user's LH information qualifies as "contents" within that statutory definition. Google's users employ LH to record where they have been and when. In doing so, they "transfer" signals and data to Google, *id.* § 2510(12)—data that Google processes to fill users' Timelines and compile an accurate record of users' whereabouts, among other things. The user's location itself is the "substance" and "meaning" of the data the user transfers to Google, *id.* § 2510(8). The user's locations and movements are the "substance, purport, [and] meaning" of the data transmitted and they fill the digital journal that the Timeline feature provides. Although the contents of that journal are reflected on a map in one's Google account rather than in a written document, the locations and travels recorded therein are fundamentally the contents of the journal, capable of being reviewed, edited, and deleted by the user. Such information is plainly "contents" under the Act.

To be sure, location-reporting data in other contexts is sometimes considered to be "records" of electronic communications (sometimes called "metadata") because it is transmitted incidentally to a user's interaction with his or her mobile device. Sending such location data to a third party, in other words, is sometimes an ancillary byproduct of using a mobile device for other purposes (*e.g.*, to make a call or to find the best route home). That is certainly true of CSLI. As the Supreme Court explained in *Carpenter*, CSLI is generated "[e]ach time the phone

connects to a cell site," which can occur "several times a minute" in order to maintain the phone's function. 138 S. Ct. at 2211; *see also Graham*, 824 F.3d at 433 ("CSLI is non-content information because 'cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves.'"). As the Third Circuit has explained, however, location data need not be ancillary to an electronic communication; often, location data "serves no routing function, but instead comprises part of a communication's substance" itself. *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 136 (3d Cir. 2015). The question is whether the location information serves as "dialing, routing, addressing, or signaling information," or whether, as here, such information is "part of the substantive information conveyed to the recipient"—in which case "by definition it is 'content.'" *Id.*; *see also id.* at 137; *In re Certified Question of Law*, 858 F.3d 591, 594 (Foreign Int. Surv. Ct. Rev. 2016) (holding that digits an individual enters on a dial pad after dialing a telephone number, such as a PIN or a bank account number, qualify as content information because they transmit substantive information).[11] When users convey their locations to Google to save and store using the LH service, the data is not performing a "routing" or "addressing" role; it is itself the "substantive information" of the user's communications, 806 F.3d at 137, and thus "contents" for the purpose of the SCA.

Because LH information is "contents" under the SCA, the government must generally obtain a warrant to compel Google to disclose it—just as it would have to do to compel Google to produce the contents of a user's written journals stored on Google Drive. *See* 18 U.S.C.

[11] *See also* Orin Kerr, Volokh Conspiracy, Wash. Post, *Websurfing and the Wiretap Act* (June 4, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/ ("the line between contents and metadata is not abstract but contextual with respect to each communication").

§ 2703(a), (b)(1)(A); *Warshak*, 631 F.3d at 288. Thus, regardless of the Fourth Amendment analysis, the government was required to obtain a warrant in this case and to satisfy all the substantive and procedural obligations attending the issuance of a warrant.

III. ABSENT AN APPLICABLE EXCEPTION, THE FOURTH AMENDMENT REQUIRES THE GOVERNMENT TO OBTAIN A WARRANT TO COMPEL PRODUCTION OF "LOCATION HISTORY" INFORMATION

The Constitution also required a warrant in this case. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const., amend. IV. The Amendment's purpose "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Camara v. Municipal Court*, 387 U.S. 523, 528 (1967). The Fourth Amendment protects people against unreasonable "searches," and governmental action that intrudes upon an "expectation of privacy" that "society is prepared to recognize as 'reasonable'" constitutes a search. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Because the government's acquisition of Google LH information via a geofence request intrudes upon just such a reasonable expectation of privacy, it constitutes a search for which a warrant is generally required.

Under the traditional *Katz* analysis, Google's users have a reasonable expectation of privacy in their LH information. Google LH information "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'"—what the Supreme Court described in *Carpenter* as "the privacies of life." 138 S. Ct. at 2217 (quotation marks omitted). The Court in *Carpenter* held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured" through the government's acquisition of cell-site location information. *Id.* The same is true of Google LH information.

The question in *Carpenter* was "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." 138 S. Ct. at 2211. As the Supreme Court explained, access to such records implicates two lines of precedent: one addressing "a person's expectation of privacy in his physical location and movements" and the other "draw[ing] a line between what a person keeps to himself and what he shares with others." *Id.* at 2215-2216. The government's ability to obtain CSLI plainly implicated a person's "reasonable expectation of privacy in the whole of [his] physical movements." *Id.* at 2217. By obtaining historical location data generated by a person's cell phone, the Court explained, the government could obtain "an all-encompassing record of the holder's whereabouts," thus "revealing not only his particular movements" but the most intimate details of his or her life, *id.* at 2217-2218; *see also Riley v. California*, 573 U.S. 373, 403 (2014) ("With all [modern cell phones] contain and all they may reveal, they hold for many Americans 'the privacies of life.'"). And while it was true that cell-phone-generated location information was shared with a third party (the cellular provider), the Court reasoned, that did not diminish users' reasonable expectation of privacy in that information, given that it constituted—in essence—"a detailed chronicle of a person's physical presence compiled every day [and] every moment." *Carpenter*, 138 S. Ct. at 2220; *see also United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements…."); *United States v. Aigbekaen*, 943 F.3d 713, 723 (4th Cir. 2019) (referring to location history as "unusually sensitive").

The same factors that led the Court in *Carpenter* to find a reasonable expectation of privacy in historical CSLI apply just as forcefully to Google LH information. Google LH information, like the CSLI at issue in *Carpenter* and the GPS data in *Jones*, permits the

government to ascertain where a person has been and when—contravening the person's "legitimate expectation of privacy in the record of his physical movements." 138 S. Ct. at 2217. As was true of the CSLI at issue in *Carpenter*, by compelling Google to disclose LH information, the government can, "[w]ith just the click of a button," access a "deep repository of historical location information at practically no expense." *Id.* at 2218. Such data is remarkably revealing. Like CSLI, Google LH information lets the government "travel back in time to retrace a person's whereabouts." *Id.* In fact, the LH information at issue here is significantly more granular than the data at issue in *Carpenter*. The CSLI at issue there allowed the government to trace a suspect to an area that could have been as wide as four square miles. *Id.*; *see also id.* at 2232 (Kennedy, J., dissenting). By contrast, the information recorded in a Google user's LH information potentially records a person's whereabouts to within a matter of meters. *See supra* p. 10. The privacy interests implicated by Google LH information are thus even greater than in *Carpenter*.[12]

Here, the government argues—just as it did in *Carpenter*—that users have no reasonable expectation of privacy in their Google LH information because such records consist only of data that users have "revealed to a third party." Opp. 9. But the Supreme Court rejected that argument in *Carpenter*, and this Court should do the same here. The so-called third-party

[12] As noted, each individual estimate of a user's location reflected in the LH service has a margin of error, which distinguishes it from CSLI. *See supra* n.7. But that does not undermine the fact that a user has a reasonable expectation of privacy in her location as it is reflected in LH information—especially given that such information draws on data that can be far more precise than is CSLI and is highly reliable in context. At the same time, the margin of error associated with LH data means that the government's effort to use this information for purposes for which the LH service was not designed creates a likelihood that the LH data will produce false positives—that is, that it will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there. That, in turn, means that the potential incursion on privacy is quite significant indeed.

doctrine, as the Court explained in *Carpenter*, traces its roots to *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979)—cases in which the government obtained "business records" of a defendant's bank (in *Miller*) and telephone company (in *Smith*) that revealed personal information about the defendants. In each case, the Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," *Smith*, 442 U.S. at 743-744, and concluded that no search had occurred. But the Supreme Court in *Carpenter* conclusively rejected the argument that the doctrine should extend to CSLI. 138 S. Ct. at 2219-2220. For one, the Court explained, "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information" collected today by third parties of all kinds. *Id.* at 2219; *cf. United States v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007) (individuals have a reasonable expectation of privacy in the contents of their text messages). For another, the Court reasoned, "the second rationale underlying the third-party doctrine"—voluntary exposure—did not justify the application of the doctrine to CSLI, given that, for multiple reasons, users did not genuinely "share" such data with phone companies. *Carpenter*, 138 S. Ct. at 2220.

Neither of the two "rationale[s] underlying the third-party doctrine" justifies extending that doctrine to the LH information here. *Carpenter*, 138 S. Ct. at 2219-2220. First, it is not the case that Google users have a "reduced expectation of privacy" in LH information. *Id.* at 2219. As described above, LH functions in effect as a daily journal of a user's whereabouts and movements with a potentially high degree of precision. It can reveal when a user was at her home (or someone else's), a doctor's office, a place of worship, a political meeting, or other sensitive locations. The information is far more revealing than the bank records or telephone pen

register information at issue in *Smith* and *Miller*, and users expect that information to remain private. *See supra* pp. 6-10.

Second, as in *Carpenter*, the fact that users voluntarily choose to save and share LH information with Google does not on its own implicate the third-party doctrine, to the extent that doctrine is still viable. 138 S. Ct. at 2220.[13] The Court in *Carpenter* emphasized that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.* (quoting *Riley*, 573 U.S. at 385). For many users, the same is true of the location-based "services that [cell phones] provide," *id.*—including the ability to track one's own movements and enrich one's electronic footprint with that information. Moreover, unlike the business records of the third-party bank and telephone company in *Smith* and *Miller*, LH information is not compiled "for … business purposes" by the third party, *Smith*, 442 U.S. at 743—the key factor that justified the development of the doctrine in the first place. Rather, it is created and stored at the discretion of the user for the user's own purposes and remains in the user's control. Such relationships are common in the digital age. In *Warshak*, for instance, the fact that individuals transmitted their emails to a third party did not stop the court from finding that those individuals enjoyed a reasonable expectation of privacy in the contents of their emails. *See Warshak*, 631 F.3d at 288 (rejecting the applicability of the third-party doctrine and explaining that "the best analogy" was "cases in which a third party carries, transports, or stores property for another"—cases in which "the customer grants access to the [provider] because it is essential to the customer's interests"). The same is true here.

[13] *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (observing that the third party doctrine espoused by *Smith* and *Miller* is "ill suited to the digital age").

The government alternatively argues that *Carpenter* does not apply because the request here applied to a supposedly small area and a shorter period of time than the CSLI requests in *Carpenter*. Opp. 6-8. But there is nothing limited about a geofence search. As explained, *see supra* pp. 12-13, in order to conduct such a search, Google must search across the records of the account holders who entrust Google with their personal LH information. That is a significant incursion on privacy. Unlike the CSLI requests in *Carpenter*, moreover, which rested on the government's belief that particular suspects were involved in a crime—and which sought information only for those users—when the government seeks LH information via a geofence request, it does not know whose records it is searching for. The result is that the government obtains information associated not only with a specific person of interest whose actions might have given rise to probable cause or at least reasonable suspicion, but for numerous others who happened to have LH information from the area. The government's comparison to a "tower dump" (Opp. 8) fails for essentially the same reasons. A tower dump entails a search of records relating only to those mobile devices that were present in the defined area at the defined time; a geofence request requires a search across all Google users for their LH information. And a tower dump yields data that is significantly less granular than a user's LH.

Ultimately, although the time period covered by the warrant here is shorter than the CSLI requests in *Carpenter*, that distinction does not defeat Google's users' reasonable expectation of privacy. A shorter timeframe could make a dispositive difference when dealing with CSLI or tower dump information because a snapshot of such data, if sufficiently limited in duration, would not result in "a detailed and comprehensive record of the person's movements." *Carpenter*, 138 S. Ct. at 2217. It would reveal only that a particular device was at a particular place at one narrow point in time. But because of its greater granularity and precision, a Google

user's LH information allows the government to reconstruct a "detailed and comprehensive record of [the user's] movements," even if only for an hour or two—something that law enforcement would not be able to do using traditional investigative methods. *Id*. at 2217.

A request compelling production of Google LH information accordingly constitutes a search within the meaning of the Fourth Amendment. Unless an exception applies, the government thus "must generally obtain a warrant supported by probable cause before acquiring such records." *Carpenter*, 138 S. Ct. at 2221.

CONCLUSION

Google takes no position on whether the warrant in this case satisfies the requirements of probable cause and particularity or, if it does not, whether suppression is appropriate. But in resolving those questions, the Court should take into account the complete factual and legal context, and it should hold that both the SCA and the Fourth Amendment require the government to obtain a warrant to compel Google to search LH information via a geofence search. That result is compelled by the statute and the Constitution and the cases applying them. It is also the only result that takes appropriate account of the singularly broad and intrusive nature of a geofence search and the granularity of the intimate detail it produces. Given the capacity of geofence searches to intrude on personal privacy, their use should be supervised by a neutral magistrate and restricted to cases in which the government can establish probable cause.

Dated: December 20, 2019

Respectfully submitted,

/s/ Brittany Blueitt Amadi
Brittany Blueitt Amadi (Va. Bar No. 80078)
Catherine Carroll (Va. Bar. No. 50939; *pro hac vice* pending)
Alex Hemmer (*pro hac vice* pending)
WILMER CUTLER PICKERING HALE AND DORR LLP
1875 Pennsylvania Ave. NW
Washington, DC 20006
Tel: (202) 663-6000
Fax: (202) 663-6363
brittany.amadi@wilmerhale.com
catherine.carroll@wilmerhale.com
alex.hemmer@wilmerhale.com

Counsel for Amicus Google LLC

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

UNITED STATES' RESPONSE TO AMICUS CURIAE BRIEF OF GOOGLE LLC

The United States of America, by its undersigned attorneys, submits this response to the Amicus Curiae Brief of Google LLC. (ECF No. 59-1.)

ARGUMENT

I. THE DEFENDANT VOLUNTARILY CONVEYED HIS LOCATION INFORMATION TO GOOGLE.

Google confirms that the defendant voluntarily conveyed his location information to Google, even under the demanding standard for voluntary disclosure used by the Supreme Court in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *Carpenter* held that cell-site information was not voluntarily conveyed to the phone company because it was collected "without any affirmative act on the part of the user beyond powering up," because there was "no way to avoid leaving behind a trail of location data," and because carrying a cell phone was "indispensable to participation in modern society." *Id.* at 2220. Google's description of how its location services function demonstrates that these factors do not apply to the Location History information obtained by investigators here.

First, Google details the multiple steps the defendant was required to take for Google to collect and store his Location History information:

> [Location History] functions and saves a record of the user's travels only when the user opts into [Location History] as a setting on her Google account, enables the "Location Reporting" feature for at least one mobile device, enables the device-location setting on that mobile device, permits that device to share location data with Google, powers on and signs into her Google account on that device, and then travels with it.

ECF No. 59-1 at 8. Thus, Google's storage of the defendant's location information took far more than him powering up his cell phone: he had to affirmatively opt in multiple times to enable Google's collection and storage of his Location History information.

Second, Google confirms that even after the defendant chose to have Google store his location information, he retained the ability to delete it: "[t]he user can review, edit, or delete her Timeline and [Location History] information from Google's servers at will." ECF No. 59-1 at 8. Thus, the defendant could have avoided having Google store his location information, unlike the cell-site information in *Carpenter*.

Third, Google's description of its location services makes clear that having Google store Location History information is not indispensable to participation in modern society. As an initial matter, Google states that "many of Google's products and services can be used without a Google account." ECF No. 59-1 at 5. Google Search is quite useful, but one need not have a Google account to use Google Search. In contrast, the benefits Google describes from enabling Location History seem minimal. According to Google, these benefits for an account holder include the ability to "obtain personalized maps or recommendations based on places she has visited, get help finding her phone, and receive real-time traffic updates about her commute," as well as "the ability to track one's own movements and enrich one's electronic footprint." ECF No. 59-1 at 6-7, 22. Access to such features is far from indispensable.

In sum, the defendant voluntarily disclosed his Location History information to Google because he opted in to its collection and storage, because he had the ability to edit and delete it, and because its collection and storage by Google is not indispensable to participation in modern society. Google is correct when it states that the defendant "errs in asserting that '[i]ndividuals do not voluntarily share their location information with Google.'" ECF No. 59-1 at 9.

II. THE DEFENDANT HAD NO REASONABLE EXPECTATION OF PRIVACY IN TWO HOURS OF GOOGLE LOCATION HISTORY INFORMATION.

The Supreme Court "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976). This principle did not control in *Carpenter* because the Court concluded that cell-site information "is not truly 'shared' as one normally understands the term." *Carpenter*, 138 S. Ct. at 2220. In addition, *Carpenter* held only that "accessing seven days of [cell-site information] constitutes a Fourth Amendment search." *Id.* at 2217 n.3. Here, the defendant voluntarily conveyed his location information to Google under the reasoning of *Carpenter*, and investigators obtained only two hours of that information, rather than a "comprehensive chronicle of the user's past movements." *Id.* at 2212. Google's disclosure of location information therefore was not a Fourth Amendment search.

Google's arguments that disclosure of two hours of the defendant's location information was a Fourth Amendment search lack merit. Google points out that Location History information is more precise than cell-site information, and it argues that Location History information therefore

implicates greater privacy interests than cell-site information. *See* ECF No. 59-1 at 10, 20. But as the United States explained in its Response Brief, the Supreme Court in *Carpenter* assumed that cell phone location information would approach the precision of GPS, so the greater accuracy of Google location information provides no basis for giving it enhanced Fourth Amendment protection. *See Carpenter*, 138 S. Ct. at 2218-19; ECF No. 21 at 8-9. In *Carpenter*, the Supreme Court found that a cell phone user had a reasonable expectation of privacy in "the whole of his physical movements." *Carpenter*, 138 S. Ct. at 2219. A two-hour interval of location information cannot meet this standard, regardless of the accuracy of individual points within the interval.

Google also argues that a warrant should be required for Location History information because when Google responds to a GeoFence warrant, it must "search across all Google users for their [Location History] information." ECF No. 59-1 at 23. Similarly, it notes that a GeoFence warrant "is not tied to any known person, user, or account." *Id.* at 11. These facts, however, do not distinguish GeoFence warrants from other forms of legal process that do not involve Fourth Amendment searches or require a warrant. For example, tower dumps are not tied to any known person, user, or account, but a tower dump is not a Fourth Amendment search. *See United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019).

Moreover, service providers commonly review large sets of customer records to produce information in response to appropriately limited legal process. For example, in the traditional telephone context, investigators use subpoenas to identify the people who placed calls to a specified telephone number. Obtaining this information is not a search under *Smith v. Maryland*, 442 U.S. 735, 742-44 (1979), which held that telephone users voluntarily convey dialed phone number information to the phone company. A phone company responding to this sort of subpoena, however, may review call records for all of its customers to find this information. *See Ameritech*

Corp. v. McCann, 403 F.3d 908, 910 (7th Cir. 2005).

Similarly, the United States often uses a "specific and articulable facts" court order issued pursuant to 18 U.S.C. § 2703(d) to compel Google to disclose identity information for subscribers who accessed their Google accounts from a specified IP address during a particular time period. Internet users have no reasonable expectation of privacy in their IP address, *see United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. June 13, 2019), so use of this investigative technique is not a search. Responding to such a court order, however, requires Google to review access records for all of its account holders. These examples demonstrate that a service provider's response to appropriately limited legal process does not become a search merely because the service provider must review a large set of records to find the responsive information.[1]

Google further asserts that the defendant retains a reasonable expectation of privacy in Google Location History information because it "is not compiled 'for . . . business purposes.'" ECF No. 59-1 at 22. As an initial matter, however, Google's Brief does not actually claim that Google does not use customer location information for its business purposes. Google states that location information is stored "primarily" for the user's benefit, ECF No. 59-1 at 8, but that formulation suggests that customer location information is also used for Google's business purposes. Google should clarify the extent to which it uses and benefits from customer location information, including both Location History information and any other Google databases that

[1] It would also be possible for Google to create an additional database of Location History information that would obviate its need to review the Location History information of all customers in response to a GeoFence warrant. Google could create a database that indexed Location History information based on its location in some sort of cellular grid. When Google received a GeoFence warrant, it would then need to review only location data from the relevant cell or cells, much like a tower dump. This possibility provides further evidence that producing GeoFence information does not become a search merely because Google reviews a large set of customer records: whether Google's production of GeoFence information constitutes a search for Fourth Amendment purposes should not depend on the internal structure of Google databases.

store location information pertaining to account holders.[2]

Moreover, even Google's limited discussion of its use of account holder location information shows that Google does in fact use that information for a "business purpose." Google compares location information to email, *see* ECF 59-1 at 22, but when an email service provider sends, receives, and stores email, it need not review or use the contents of the email. In contrast, Google's use and analysis of customer location information is essential to the location services it provides. For example, Google acknowledges that it uses account holder location information to provide "real-time traffic updates." ECF 59-1 at 7. This service requires Google to analyze location information sent to it by its customers and share the results of its analysis with other nearby customers. When a business uses information supplied by a customer to provide services, the customer retains no reasonable expectation of privacy in that information. For example, an individual retains no reasonable expectation of privacy in personal financial records shared with an accountant. *See Couch v. United States*, 409 U.S. 322, 335-36 (1973).

In addition, the principle that one retains no reasonable expectation of privacy in information revealed to a third party has never been limited to business records. For example, this principle applies to incriminating statements made in the presence of an informant. *See Hoffa v. United States*, 385 U.S. 293, 413-14 (1966). More generally, the roots of the third-party doctrine long predate *United States v. Miller* and *Smith v. Maryland*. It is an "ancient proposition of law" that the public "has a right to every man's evidence." *United States v. Nixon*, 418 U.S. 683, 709 (1974). The Supreme Court has recognized that "as early as 1612, . . . Lord Bacon is reported to have declared that 'all subjects, without distinction of degrees, owe to the King tribute and service,

[2] Google states that "[Location History] information was the only location information produced to the government in response to this geofence warrant," but it does not address whether it stores other databases containing location information. ECF No. 59-1 at 9.

not only of their deed and hand, but of their knowledge and discovery.'" *Blair v. United States*, 250 U.S. 273, 279-280 (1919) (quoting *Countess of Shrewsbury Case*, 2 How. St. Tr. 769, 778 (1612)). In this case, Google's role is fundamentally that of a witness: Google observed the location of people present at the robbery, and the government called upon it to disclose its observations. Allowing litigants to obtain information from witnesses is critical to the truth-seeking function of the justice system: "[t]he need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts." *Nixon*, 418 U.S. at 709. It was not a search when Google revealed its observations to investigators.

III. THIS COURT NEED NOT ADDRESS GOOGLE'S INTERPRETATION OF THE STORED COMMUNICATIONS ACT.

This Court need not consider Google's argument that as a statutory matter, the Stored Communications Act ("SCA") requires a warrant to compel Google to disclose location information. *See* 18 U.S.C. §§ 2701-13; ECF No. 59-1 at 14-18. Investigators in this case obtained a warrant for the defendant's location information, and his motion to suppress is based solely on his allegation of a Fourth Amendment violation, not a statutory violation. If the United States ever attempted to compel Google to disclose GeoFence information via a "specific and articulable facts" court order issued pursuant to 18 U.S.C. § 2703(d), Google would then have the opportunity to challenge that order.

Another reason why this Court need not consider the SCA here is because the SCA provides no suppression remedy for a statutory violation. The SCA includes criminal penalties and civil damages for certain types of violations of the SCA, *see* 18 U.S.C. §§ 2701 & 2707, and it further specifies that "the remedies and sanctions described in this chapter are the only judicial

remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. Courts have thus held that statutory violations of the SCA do not result in suppression. *See United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014) ("suppression is not a remedy for a violation of the [SCA]"); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) ("the [SCA] expressly rules out exclusion as a remedy"). Thus, even if the defendant were to allege a violation of the SCA here, the appropriate focus for this Court would still be the defendant's Fourth Amendment argument.

The United States notes, however, that there is some reason to doubt Google's analysis of how the SCA applies to Google location information. For one example, Google argues that under the SCA, Google location information "qualifies as 'contents' of 'electronic communications.'" ECF No. 59-1 at 16. But Google selectively quotes only a portion of the definition of "electronic communication." Google states: "The SCA defines an 'electronic communication' as a 'transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part' by an electronic system.'" *Id.* (quoting 18 U.S.C. § 2510(12)). Google ignores a potentially significant exclusion from this definition: the definition excludes "any communication from a tracking device (as defined in section 3117 of this title)." 18 U.S.C. § 2510(12)(C). Google elsewhere states that Google's location services give one "the ability to track one's own movements," which suggests that a user who opts in to Google Location History may be using a tracking device. *See* 18 U.S.C. § 3117 (defining a "tracking device" to mean "an electronic or mechanical device which permits the tracking of the movement of a person or object"). If the location information users send to Google is a communication from a tracking device, the location information could not be the contents of an electronic communication. Again, however, because interpreting the SCA is not necessary to resolve the defendant's suppression motion, this Court

should not address the SCA here.

CONCLUSION

Google confirms that the defendant voluntarily conveyed his location information to Google. This Court should deny the defendant's motion to suppress the fruits of the GeoFence warrant.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 10th day of January, 2020, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koeing
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorneys
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

DEFENDANT'S RESPONSE TO GOOGLE'S MOTION TO FILE AMICUS CURIAE BRIEF IN SUPPORT OF NEITHER PARTY

Okello Chatrie, through counsel, responds as follows to Google's motion to file an *amicus* brief in support of neither party:

INTRODUCTION

On December 20, 2019, Google moved this Court to file an *amicus* brief in support of neither party, ECF No. 59, and included its proposed 24-page brief as an attachment. ECF No. 59-1. Mr. Chatrie recognizes Google's interest in this case and appreciates the additional context that Google presents in its brief. Most of the new information that Google proffers strongly supports Mr. Chatrie's motion to suppress evidence obtained from a "geofence" general warrant, *see* ECF No. 29, including the limitless breadth of the search involved and Google's handling of Location History information as communications content akin to a "virtual journal." *Id.* at 6.

Nonetheless, Google seeks to bolster the degree of voluntariness involved in keeping such a journal, giving the misleading impression that such data collection is always, or even generally, informed and intentional. Furthermore, the information Google has provided is incomplete. The defense has requested in discovery information on the categories of data Google collected, stored, and provided to law enforcement, as well as the specific inputs and algorithms used to produce the

responsive Location History data in this case. Google addresses some but not all of these issues in its brief, seeming to pick and choose what it wishes to address.

Consequently, Mr. Chatrie must object to the Court's consideration of Google's brief without further opportunity to obtain discovery from Google and examine Google representatives capable of providing answers to the legal and factual questions raised by their brief. A thorough understanding and examination of the technology at issue here is essential to the full and fair resolution of the significant constitutional issues raised by this case. Google has already demonstrated its willingness to participate in these proceedings. This Court should require its future participation as necessary to assess to the accuracy of the new facts it seeks to interject, or alternatively, to reconsider the motion to participate as *amicus*.

ARGUMENT

I. Google's Brief Supports Mr. Chatrie's General Warrant & Search Arguments

Google distinguishes the geofence warrant at issue here from other types of law enforcement requests, emphasizing that it requires a uniquely broad search of all Google users' timelines. *See* ECF No. 59-1 at 11. Whereas typical requests compel Google to disclose information associated with a specific user, "[g]eofence requests represent a new and increasingly common form of legal process that is not tied to any known person, user, or account." *Id*. Even so-called "tower dumps" are more limited in scope than geofence warrants. As Google explains, a tower dump "requires a provider to produce only records of the mobile devices that connected to a particular cell tower at a particular time." *Id*. at 14. As a result, the number of people directly affected by a tower dump has an upper limit, *i.e.*, the number of devices actually present in the area. By contrast, a geofence search has no such cap because "Google has no way to identify which of its users were present in the area of interest without searching the [location history] information

stored by every Google user." *Id*. In other words, the initial stage of *any* geofence warrant necessarily entails searching *every* user for whom Google has location history data.

Google's explanation of the search process supports Mr. Chatrie's argument that geofence warrants are unconstitutional general warrants. As Mr. Chatrie contends, geofence warrants are overbroad and lack particularity because they "authorize the search of an unlimited number of people's location data," ECF No. 48 at 4, rendering them unconstitutional from the outset. *See also* ECF No. 29 at 16-24. Regardless of how many devices Google initially identifies—be it 9, 19, or 9,000—the process of doing so is the same: "Google must search across all [Location History] journal entries to identify users with potentially responsive [Location History] data, and then run a computation against every set of coordinates to determine which [Location History] records match the time and space parameters in the warrant." ECF No. 59-1 at 12-13. There is no probable cause to justify such a boundless search, and the discretion it affords to both Google and the government demonstrates a profound lack of particularity. Such a warrant is no warrant at all, but an unconstitutional general warrant. *See* ECF No. 29 at 17-21.

Google's description of Location History information as a personal "journal" further reinforces this conclusion. *See* ECF No. 59-1 at 6. Google states that Location History information is not a "business record" in any traditional sense, but "is essentially a history or journal that Google users can choose to create, edit, and store to record their movements and travels." *Id*. Thus, from Google's perspective, it is akin to email stored on Google's Gmail service or personal documents stored remotely on Google Drive. *Id.* at 9, 17. Google asserts that it "is stored with Google primarily for the user's own use and benefit," *id.* at 9, and as a result, treats it as communications "contents" for purposes of the Stored Communications Act. *Id.* at 16-17.

In this light, Google functions as a trusted bailee of location history information that is created by and belongs to individual Google users. Thus, as Mr. Chatrie contends, his location information is his personal property—his own papers and effects—even though Google may be responsible for collecting and maintaining it. *See* ECF No. 29 at 15; *see also Ex parte Jackson*, 96 U.S. 727, 733 (1878) (finding a Fourth Amendment interest letters entrusted to mail carriers). Google, in turn, owes a duty to Mr. Chatrie to keep his location data safe and not disclose it to others. *See, e.g.*, 18 U.S.C. § 2702(a)(1) and (2) (prohibiting service providers from voluntarily divulging the contents of communications); Google, Privacy Policy (Dec. 19, 2019), https://policies.google.com/privacy?hl=en-US#infosharing (describing the limited circumstances in which Google will disclose user data). As Justice Gorsuch recognized in *Carpenter v. United States*, the Fourth Amendment protects one's papers and effects that are held by a third party through such a bailment. 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting) ("Whatever may be left of *Smith* and *Miller*, few doubt that e-mail should be treated like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest."). Likewise, Justices Kennedy, Thomas, and Alito all acknowledged that the third-party doctrine should not apply where businesses are the bailees or custodians of records with a duty to hold them for a defendant's use. *Id.* at 2228, 2230 (Kennedy, J., dissenting).

By compelling Google to turn over Mr. Chatrie's location history, the government infringed on his property interest in that data. Such a trespass constitutes a Fourth Amendment search and seizure, just as surely as if the government had searched and seized papers in Mr. Chatrie's hotel room or safety deposit box. *See Stoner v. California*, 376 U.S. 483, 490 (1964) ("[A] guest in a hotel room is entitled to constitutional protection against unreasonable searches and seizures."); *Couch v. United States*, 409 U.S. 322, 337 (1973) (Brennan, J., concurring)

(suggesting that individuals have a reasonable expectation of privacy in the contexts of a safety deposit box).

In this case, however, the government went even further. The geofence warrant here is the digital equivalent of searching every safety deposit box in every branch of a global bank to find one piece of stolen property. Yet any warrant purporting to authorize such a search would be an impermissible general warrant, void as a basic principle of both English common law and the Fourth Amendment. *See, e.g.*, William Hawkins, 2 *A Treatise of the Pleas of the Crown* 84 (Professional Books 1973) (P.R. Glazebrook, ed) ("I do not find any good Authority, That a Justice can justify sending a general Warrant to search all suspected Houses in general for stolen Goods, because such Warrant seems to be illegal in the very Face of it"); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding that a warrant to search all suspected places, stores, shops and barns in town for stolen goods was an unlawful general warrant). The same principle applies here. Google's analogy to personal journals simply underscores the property rights affected by a geofence request and highlights the impermissibility of a general warrant authorizing the search of all such data.

II. Enabling Location History Does Not Defeat Mr. Chatrie's Expectation of Privacy in His Data

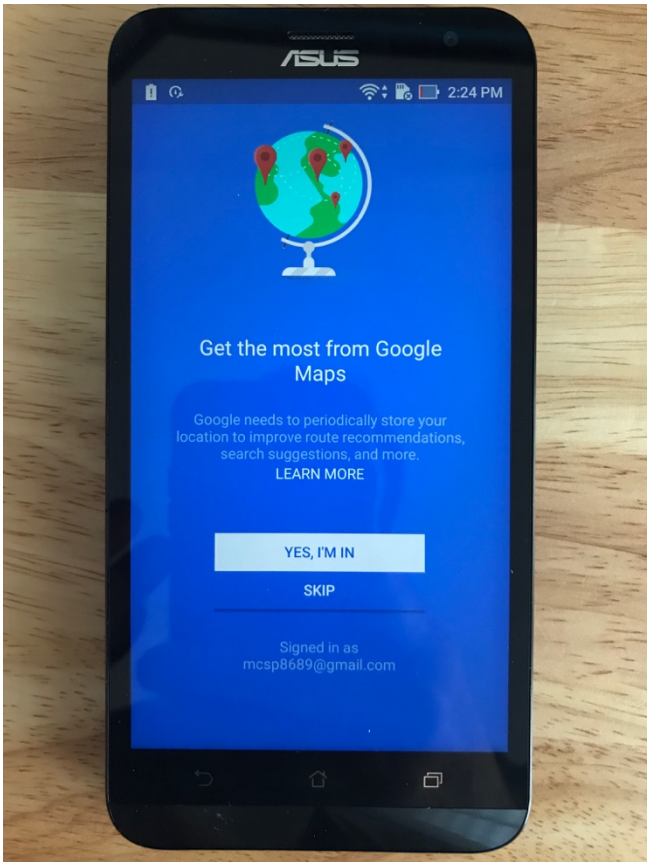
Although Mr. Chatrie appreciates Google's comparison of Location History information to a personal journal, it is not at all clear that it is a journal most people intend to keep. Google points to the account settings users must enable for the Location History service to function, claiming that the defense "errs in asserting that '[i]ndividuals do not voluntarily share their location information with Google,' . . . and that the acquisition of user location records by Google is 'automatic and inescapable.'" ECF No. 59-1 at 9. But in practice, the process for enabling Location History is not nearly as deliberate or informed as Google's brief may lead one to believe.

Google states that Location History will function only when a user takes multiple affirmative steps to enable it. According to Google, a user must (1) opt into Location History as a setting; (2) enable the "Location Reporting" feature; (3) enable the device-location setting; (4) permit location sharing with Google; (5) power on the device and sign into Google; and (6) travel with the device. *Id.* at 8. Yet virtually all of these steps may be accomplished in the first few moments of setting up and using a new device, such as the Samsung Galaxy S9 used by Mr. Chatrie, while the full consequences of doing so would not be apparent the ordinary user.

The Samsung Galaxy S9 is a mobile device that uses Google's Android operating system. As a result, one of the very first steps in setting up an S9 is to log into or create a Google account, the prompts for which appear prior to even creating a passcode for the device. *See, e.g.*, Tech ARP, *Setting Up The Samsung Galaxy S9 For The First Time*, YouTube (Mar. 8, 2018), https://www.youtube.com/watch?v=n-giid2lc_4. While it is possible to skip this step, attempting to do so yields a pop-up warning from Google that doing so will prevent the user from: downloading apps, music, and games; syncing services like Calendar and Contacts; or activating "device protection" features. *Id*. In short, most of the features commonly associated with a modern mobile device, apart from voice calls and web browsing, would be unavailable to an ordinary user who does not log into a Google account. As a result, requirement (5) is quickly satisfied without any reference to Location History. Moreover, the S9 comes out of the box with the device-location setting enabled, satisfying requirement (3). Disabling this setting renders the device incapable of many basic functions.

Requirements (1), (2), and (4) are likely to occur simultaneously when opening an application like Google Maps for the first time. When setting up an Android device similar to the S9, the defense immediately encountered a full screen from Google prompting the user to "Get the most from Google Maps," which states only that "Google needs to periodically store your location to improve route recommendations, search suggestions, and more." A button reading "YES I'M IN" is highlighted while options to "SKIP" and "LEARN MORE" were not.

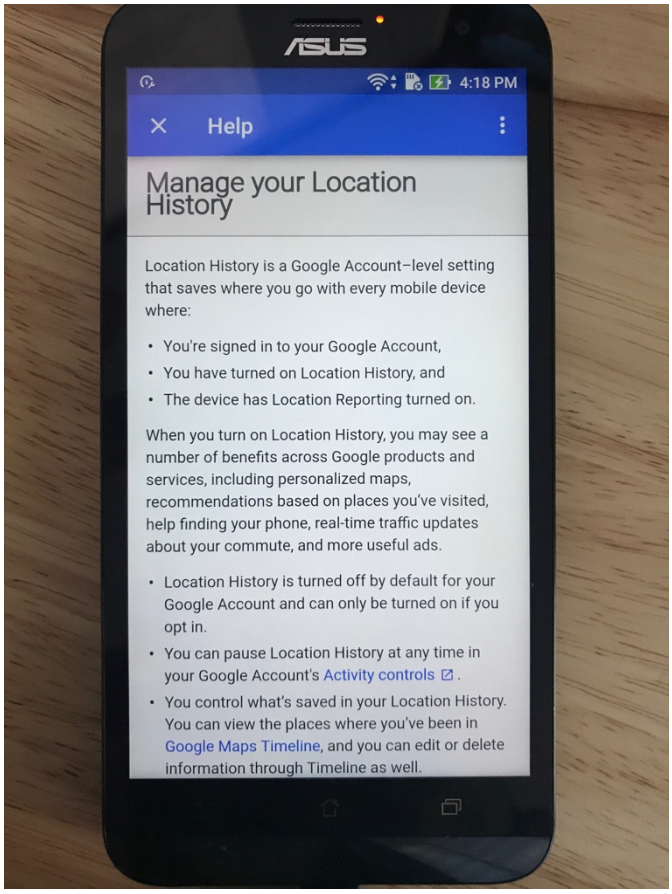
Figure 1



Clicking "YES I'M IN" enabled Location History and turned on Location Reporting, apparently satisfying both requirements (1) and (2), despite the fact that neither Location History nor Location Reporting are mentioned by name. The "LEARN MORE" section informs users that their location information will be reported to Google by enabling Location History, presumably satisfying requirement (4) at the same time. Significantly, there appears to be no way to enable Location History without also enabling Location Reporting and permitting location sharing with Google. In short, requirements (1), (2), and (4) are not independent requirements, but part and parcel of a single click. Consequently, after just the first few minutes on a new Android device like the S9, most users will have accomplished steps (1)-(5)—simply by setting it up, opening Maps, and following Google's prompts. All that remains is to move around in order to satisfy requirement (6).

Critically, the full consequences of taking these initial steps is likely not apparent to the ordinary user. There is nothing in the on-screen prompts to indicate that tapping "YES, I'M IN" will start a log of every step a user takes and share it with Google. It does not mention Location History or Location Reporting explicitly. And while the "LEARN MORE" section mentions "Google Maps Timeline" as a way to "view the places where you've been," it does not elaborate. Instead, Google takes that opportunity to explain why users should enable Location History, stating: "When you turn on Location History, you may see a number of benefits across Google products and services, including personalized maps, recommendations based on places you've visited, help finding your phone, real-time traffic updates about your commute, and more useful ads." When presented with the option in this fashion, it is easy to see how users may enable Location History without realizing the full implications of their decision.

Figure 2



Consequently, Google's description of the opt-in process for Location History does not accurately reflect the user experience, making it appear as if the decision is more intentional and informed than it really is. This raises significant doubt about the degree to which enabling Location History is truly informed and voluntary, as Google's six requirements may be quickly and easily satisfied without any mention of Location History or Location Reporting. Rather, ordinary users

like Mr. Chatrie are very likely to be unaware that Location History is on. Even computer security experts have reported not realizing that the feature had been enabled. *See, e.g.*, Matt Boddy, *The Google tracking feature you didn't know you'd switched on*, Naked Security (Oct. 3, 2017), https://nakedsecurity.sophos.com/2017/10/03/the-google-tracking-feature-you-didnt-know-youd-switched-on/. In this sense, Location History is effectively "inescapable and automatic" for ordinary Google users.

Even if enabling Location History requires a weak affirmative step, Mr. Chatrie still maintains a reasonable expectation of privacy in his data. All cell phone users, for example, must agree to share their cell site location information with the phone company, pursuant to the company's terms of service and as required for the phone to function. But doing so does not waive their Fourth Amendment protection in that data, as the intended scope of that sharing is limited accordingly. As the Florida Supreme Court recognized in *Tracey v. State*, conveying personal information to a third party for personal purposes cannot be considered disclosure for all purposes, especially to parties who were not involved in the transaction. 152 So. 3d 504, 522 (Fla. 2014). Simply because a user knows that the service provider detects his location "for call routing purposes, and which enable cell phone applications to operate for navigation, weather reporting, and other purposes, does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes." *Id.*; *see also Carpenter*, 138 S. Ct. at 2219 (citing *Riley v. California*, 573 U.S. 373, 392 (2014)). Consequently, Mr. Chatrie had an expectation of privacy in his Location History information that he did not forfeit by conveying it to Google for his personal use.

Finally, Google asserts that it disclosed only an "anonymized" list of user accounts in steps one and two of the geofence warrant process. *See* ECF No. 59-1 at 12-13. But as Mr. Chatrie

argues, "[t]he fact that Google masks the true "Device ID" with a pseudonym does not make the data anonymous." *See* ECF No. 68 at 3. Precise geolocation information is "inherently identifiable," capable of revealing "each person's unique path through life." *Id.*; *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1716 (2010) (compiling computer science research showing that it is possible to "reidentify" or "deanonymize" individuals from ostensibly anonymous data). As a result, the Court should not discount the intrusiveness of the initial data returns disclosed by Google. Had the government obtained the contents of user emails but asked Google to redact the to/from information, there would be no doubt that a search had still occurred. The same holds true for geolocation information.

III. Google's Brief Raises More Questions Than It Answers, Requiring Further Discovery from Google

In moving this Court to participate as *amicus*, Google acknowledges that it is no mere observer. Instead, because of its role in executing the geofence warrant, Google recognizes that it is "well situated to explain the nature of the data and the steps Google takes in response to geofence warrants like the one at issue here." ECF No. 59-1 at 2. In fact, as Mr. Chatrie argues in support of further discovery, Google functioned as "a private actor participating in a specific criminal investigation at the behest of the government." ECF. No. 49 at 2. And as a result, the defense maintains that Google's direct and central role in the search and seizure of Mr. Chatrie's data has made it a part of the investigative team and subject to discovery. *Id*. at 2-3.

By participating as *amicus*, however, Google seeks to pick and choose which information to disclose. Some of the information in Google's brief is responsive to Mr. Chatrie's discovery request. *See* ECF No. 28. But at the same time, some answers are conspicuously absent. Mr.

Chatrie therefore requests that the Court order Google to provide further discovery to the defense or else reconsider its order granting Google's motion to participate as *amicus*.

Clear answers to Mr. Chatrie's discovery requests are material to his defense because "there is a reasonable probability" that if they are "disclosed to the defense, the result of the proceeding [will be] different." *See United States v. Bagley*, 473 U.S. 667, 682 (1985). Under Rule 16, each are material because "there is a strong indication" that each "will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *See United States v. Caro*, 597 F.3d 608, 621 (4th Cir. 2010).

A. Sensorvault, Location Services, and Web & App Activity

Two sets of unresolved factual issues about Google's response to the geofence warrant remain unanswered by Google's brief. The first set concerns what categories of data Google collected, stored, and then provided to law enforcement. Mr. Chatrie requested "[d]etails concerning Google's Sensorvault," such as "how the location data is captured and collected," "how often Google collects location data" on Android and non-Android phones, and "how many individuals' tracking information is in the Sensorvault." ECF No. 28 at 2-3. He also requested information on any "data that Google initially determined to be potentially responsive to the warrant" but ultimately excluded." *See id*. at 4. However, Google's brief did not mention Sensorvault or the other categories of location information it collects, such as Web & App Activity. ECF No. 59-1. These facts are material because they illustrate Google's cooperation with law enforcement and speak to the geofence warrant's overbreadth and lack of particularity and probable cause.

Google collects location data from users through several mechanisms, of which Location History is only one—Web & App Activity, for example, is a separate category of location data, as

is Google Location Services. ECF No. 28 at 4-5; ECF No. 48 at 6-7. The geofence warrant required Google to turn over "[d]ata" on "each type of Google account that is associated with a device that was inside the geographical area" described in the warrant. ECF No. 54-1 at 4, 9. The warrant did not limit its reach to Location History information. But Google did, apparently. Google proffers that it limited step one of the search to Location History data, meaning that it did not include location data generated by Web & App Activity or other sources, contrary to the plain language of the geofence warrant. *See* ECF No. 59-1 at 12 ("In practice, although the legal requests do not necessarily reflect this limitation, such requests can only cover Google users who had LH enabled and were using it at the time in question.").

Google, however, provides no support for this assertion or rationale for why it would restrict its search to Location History data, as opposed to including Web & App Activity or Google Location Services. Instead, Google seems to be admitting that it did not fully respond to the warrant based on some sort of internal protocol. In discovery, Mr. Chatrie has requested all such policies, guidelines, and protocols, *see* ECF No. 28 at 2. In fact, Mr. Chatrie specifically requested: "Any and all Sensorvault data that Google initially determined to be potentially responsive to the warrant … but excluded from the Sensorvault data ultimately Google provided to law enforcement officials in this case, including the reason(s) for the exclusion." *Id.* at 4. The defense needs to know, for example, the extent to which this protocol was developed in conjunction with law enforcement. Information indicating that Google worked with law enforcement officials to develop this protocol would support Mr. Chatrie's argument that the geofence warrant granted too much discretion to non-judicial officers in violation of the Fourth Amendment's particularity requirement. *See* ECF No. 29 at 17-24. It also bears on Mr. Chatrie's assertion that Google was functioning as part of the prosecution team. *See* ECF No. 49 at 2-5.

At the same time, Mr. Chatrie should not be required to simply accept Google's unsupported assertion that the geofence warrant searched only Location History information. It is clear that Google collects other types of location information via Web & App Activity and Google Location Services, and the warrant appears to request all of it. But these other functions require even less informed opt-in than Location History, operating even when Location History has been disabled. *See* ECF No. 48 at 7 (Location History "is an opt-in feature but one that has no effect on the GPS, Wi-Fi, and other location data transmitted to Google through Location Services or Web & App Activity."). Indeed, the lack of informed consent to such data collection has been the subject of civil lawsuits in the United States and Australia.[1] Consequently, any location data shared through Web & App Activity or Google Location Services may be even less voluntary than the data obtained through Location History, further supporting Mr. Chatrie's Fourth Amendment arguments.

Similarly, the defense understands that Google maintains all three forms of location information in its "Sensorvault" database. *See* ECF Nos. 28 & 38; H. Comm. on Energy and Commerce, 116th Cong., Letter to Sundar Pichai (Apr. 23, 2019); Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works.*, N.Y. Times (Apr.

[1] While the merits of these civil lawsuits are not relevant to Mr. Chatrie's motions in this criminal case, both acknowledged the difference between Location History and Web & App Activity. The Northern District of California discussed how "turning 'off' Location History" does not mean "the places you go are no longer stored" by Web & App Activity. *See* Order Granting Defendant's Motion to Dismiss at 2, *In Re Google Location History Litigation*, No. 5:18-cv-05062-EJD (N.D. Cal. Dec. 19, 2019). "[T]urning 'off' Location History only prevented general location tracking." *Id*. By contrast, the Web & App Activity setting is "'on' by default and saves certain information about a user's 'activity on Google sites and apps.'" *Id*. In short, "the two settings are distinct." *Id*. *See also* Concise Statement at 9, NSD1760/2019, *Australian Competition and Consumer Comm'n. v. Google Australia* (N.S.W. Oct. 29, 2019) (alleging that "where Users had Location History turned 'off' (or 'paused') and the Web & App Activity setting turned 'on' . . . Google obtained and retained Personal Data about the User's location.").

13, 2019); Kate Cox, *Feds Reap Data From 1,500 Phones in Largest Reported Reverse-Location Warrant*, Ars Technica (Dec. 13, 2019), https://arstechnica.com/tech-policy/2019/12/feds-reap-data-from-1500-phones-in-largest-reported-reverse-location-warrant/. Google, however, does not mention Sensorvault or explain how it might segregate Location History data in order to conduct a geofence according to its protocol. Further discovery about the Sensorvault system—such as Google's own description of it, the system's access control and maintenance policies, and how much of which kind of data it contains—is therefore highly relevant and material to Mr. Chatrie's suppression argument. Indeed, the government's case for probable cause relies on statistics citing the number of Android and non-Android users that have their location data stored with Google. ECF No. 41 at 3-4. Mr. Chatrie therefore deserves an opportunity to verify these claims with Google.

B. Wi-Fi Access Point Locations and Google's Algorithms

The second set of unresolved factual issues concerns the inputs and algorithms used to produce the Location History data provided to law enforcement. Mr. Chatrie requested the "location/source" of the "WiFi access points for individuals' location tracking data," ECF No. 28 at 1, which Google did not provide. He also requested the "algorithms used in analyzing and storing the location data," and "all information about the accuracy of the location data," which Google did not provide. *Id*. at 1-3. This information is material because it speaks to the geofence warrant's overbreadth and lack of particularity.[2]

Most significantly, Google appears to have included devices in the step one warrant returns that were actually outside the 150-meter radius authorized by the geofence warrant. In this case,

[2] This information would also help to evaluate the accuracy of the location data, which may become relevant at a later stage in these proceedings. The raw data shows that the margin of error tends to be quite large for the data points based on Wi-Fi. *See* ECF No. 68 Ex. A.

multiple users appear to have been ensnared in the geofence as a result of driving close to, but outside of the 150-meter radius. If true, this fact would strengthen Mr. Chatrie's argument that the warrant was overbroad and lacked particularity. Indeed, that is why the defense requested discovery concerning the location of Wi-Fi access points known to Google, as well as the algorithm Google used to determine which devices were inside the radius and responsive to the warrant.

To wit, Google's brief contains multiple statements that the data points are "probabilistic estimates" with "a margin of error" and include not just a "set of coordinates" but "a value . . . that reflects Google's confidence in the reported coordinates." *See* ECF No. 59-1 at 10, *Id*. n.7, 13 n.8, 20 n.12. Google does not, however, explain how these estimates, margins of error, or confidence values are calculated. It does, however, recognize that these estimates may include "false positives – that is, that [they] will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there." *See* ECF No. 59-1 at 20 n.12.

The most likely explanation for these false positives has to do with the location of the Wi-Fi access points used to determine device locations. *See* ECF No. 49 at 7. "A Wi-Fi access point can be a router, switch, Ethernet cable hub, or some other device that creates a wireless local area network." *Id*. The raw data shows that some of the location data points were based on Wi-Fi but it does not provide the location of the access points themselves. ECF No. 68 Ex. A. This is significant because when locating users, Google's algorithm appears to assume that any device connected to an access point within the 150-meter radius is also located within that radius, equating the location of the access point with the location of the device remotely connected to it. This is a false assumption. A Wi-Fi access point within the radius has its own range, which may extend well beyond the 150-meter radius. *See* Bradley Mitchell, *What Is the Range of a Typical WiFi Network?*, Lifewire (Oct. 28, 2019), https://www.lifewire.com/range-of-typical-wifi-network-816564 (last

visited Jan. 9, 2020) (stating that Wi-Fi networks have an average outdoor range of 300 feet). As a result, devices connected to such a network may be falsely included in the warrant returns even though they were physically outside the geofence.

Even with inputs that Google proffers are "highly reliable in context," Google acknowledges that its algorithm may allow for a large margin of error when locating a user. *See* ECF No. 59-1 at 20 n.12. The resulting location information may still be "sufficiently precise and reliable for the purposes for which [Location History] was designed" (*i.e.*, the commercial context), but not necessarily "for purposes for which the [Location History] service was not designed" (*i.e.*, the law enforcement context). *See* ECF No. 59-1 at 10-11 n.7, 20 n.12; Andrea M. Rodriguez, et al., *Google Timeline Accuracy Assessment and Error Prediction*, 3 Forensic Sci. Res. 240, 245 (2018) (conducting experiment and finding that Google's estimated locations with margins of error have a hit ratio of 52% when using GPS and 7% when using Wi-Fi). Such inaccuracy is not just a trial issue. As Google acknowledges, it makes "the potential incursion on privacy is quite significant indeed." *See* ECF No. 59-1 at 20 n.12.

The only way to evaluate this impact is to look at the specific inputs, including the Wi-Fi access point locations, and the algorithm responsible for determining user location based on them. This information is directly relevant to Mr. Chatrie's overbreadth and particularity arguments, as it would likely show how people outside the 150-meter radius were swept into the geofence.

CONCLUSION

Google's brief supports Mr. Chatrie's argument that the geofence warrant in this case was a general warrant, devoid of the probable cause and particularity required by the Fourth Amendment, requiring suppression the search results and all fruits thereof. But because Google effectively served as a member of the investigative team in this case, and because its brief does

not fully respond to Mr. Chatrie's discovery requests, the defense requests that the Court order Google to provide further discovery to the defense or else reconsider its order granting Google's motion to participate as *amicus*.

Respectfully submitted,

OKELLO T. CHATRIE

By: _____/s/_____

Michael W. Price
NY Bar No. 4771697 (pro hac vice)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on January 10, 2020, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

This page intentionally left blank for double-sided pagination and printing

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Richmond Division (The Hon. M. Hannah Lauck)

JOINT APPENDIX

VOLUME 2 of 11 (pages 177 - 416)

JESSICA D. ABER
United States Attorney

Kenneth R. Simon, Jr., Ass't U.S. Attorney
Peter S. Duffey, Ass't U.S. Attorney
Counsel for Appellee
919 East Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400

Nathan P. Judish, Senior Counsel
Computer Crime & Intel. Property Section
Criminal Division
U.S. Department of Justice

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
Counsel for Appellant
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800

Michael W. Price, Litigation Dir.
NACDL Fourth Amendment Ctr.
1660 L Street NW, 12th Floor
Washington, DC 20036

This page intentionally left blank for double-sided pagination and printing

TABLE OF CONTENTS

VOLUME 1 (pages 1 - 176)

District Court Docket Sheet (as of Jan. 17, 2023) 1

Indictment (Sept. 17, 2019, Doc. 1) 22

Defendant's Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Oct. 29, 2019, Doc. 29) 25

Government's Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (Nov. 19, 2019, Doc. 41) 51

Defendant's Reply to Government's Response [to] Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Dec. 9, 2019, Doc. 48) 76

Exh. A (First Step 2 Request to Google) (Doc. 48-1) 98
Exh. B (Second Step 2 Request to Google) (Doc. 48-2) 100
Exh. C (Third Step 2 Request to Google) (Doc. 48-3) 102
Exh. D (Transcript, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019)) (Doc. 48-4) ..... omitted from J.A.

Government's Notice Regarding Attachment of Google Geofence State Search Warrant to Response in Opposition to Motion to Suppress (Dec. 18, 2019, Doc. 54) 104

Affidavit for search warrant and warrant, with attachments (Doc. 54-1) 107

Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant (Dec. 20, 2019, Doc. 59-1) 118

United States' Response to Amicus Curiae Brief of Google LLC (Jan. 10, 2020, Doc. 71) 148

Defendant's Response to Google's Motion to File Amicus Curiae Brief in Support of Neither Party (Jan. 10, 2020, Doc. 72) 158

VOLUME 2 (pages 177 - 416)

Transcript, Discovery Motion Hearing (Jan. 21, 2020, Doc. 81; *see* Doc. 77 (court minutes))....177

Preliminary matters....179

Def't witness Spencer McInvaille — Direct examination....193; Cross examination....283; Redirect examination....306

Argument by the defense....318
Argument by the government....332
Rebuttal by the defense....350

Court's ruling....355

Defendant's Supplemental Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (May 22, 2020, Doc. 104)....363

United States' Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (June 12, 2020, Doc. 109)....393

VOLUME 3 (pages 417 - 694)

Transcript, Suppression Motion Hearing, Day 1 (evidence) (Mar. 4, 2021, Doc. 201; *see* Doc. 198 (court minutes))....417

Preliminary matters....420

Def't witness Spencer McInvaille — Direct examination....432; Cross examination....542; Redirect examination....586

Def't witness Marlo McGriff — Direct examination....606

VOLUME 4 (pages 695 - 1070)

Transcript, Suppression Motion Hearing, Day 2 (evidence) (Mar. 5, 2021, Doc. 202; *see* Doc. 199 (court minutes)) 695

Preliminary matters 698

Def't witness Marlo McGriff, cont'd — Direct examination ..... 699; Cross examination ..... 791; Redirect examination 841

Def't witness Sarah Rodriguez — Direct examination ..... 862; Cross examination ..... 902; Redirect examination 916

Gov't witness Jeremy D'Errico — Direct examination ..... 923; Cross examination ..... 967; Redirect examination 1010

Gov't witness Joshua Hylton — Direct examination ..... 1016; Cross examination ..... 1040; Redirect examination 1063

Concluding matters 1064

VOLUME 5 (pages 1071 - 1326)

Defendant's Post-Hearing Brief on "Geofence" General Warrant (May 3, 2021, Doc. 205) 1071

Government's Response in Opposition to Defendant's Motion for Suppression (May 21, 2020, Doc. 214; *see* Doc. 207-2) 1117

Defendant's Reply to Government's Response in Opposition to Motion for Suppression (June 4, 2020, Doc. 213) 1164

Transcript, Suppression Hearing (arguments) (June 24, 2021, Doc. 217; *see* Doc. 215 (court minutes)) 1185

Argument by the defense 1187
Argument by the government 1231
Rebuttal by the defense 1313

Concluding matters 1322

VOLUME 6 (pages 1327 - 1456)

Memorandum Opinion (denying suppression motion) (Mar. 3, 2022, Doc. 220) 1327

Order (denying suppression motion) (Mar. 3, 2022, Doc. 221) 1390

Criminal Information (May 6, 2022, Doc. 224) 1391

Transcript, Change of Plea Hearing (May 9, 2022, Doc. 247; *see* Doc. 226) 1394

Plea Agreement (May 9, 2022, Doc. 228) 1428

Statement of Facts (May 9, 2022, Doc. 229) 1444

Judgment in a Criminal Case (Aug. 19, 2022, Doc. 239) 1449

Notice of Appeal (Aug. 25, 2022, Doc. 241) 1456

VOLUME 7 (pages 1457 - 1810) – DOCUMENT EXHIBITS

Exhibits Admitted at Discovery Motion Hearing (Jan. 21, 2020)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) ..... *see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) ..... *see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) ..... *see* J.A. 2093
Def't Exh. 4: Activation Video ..... omitted from J.A., available on request
Def't Exh. 5: Three Paths Video (sealed) ..... *see* J.A. 2139
Def't Exh. 6: First Step 2 Request to Google 1457
Def't Exh. 7: Second Step 2 Request to Google 1459
Def't Exh. 8: Third Step 2 Request to Google 1461

Def't Exh. 9: Step 3 Request to Google 1463

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) .....*see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) .....*see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) .....*see* J.A. 2093
Def't Exh. 5: Three Paths Video (sealed) .....*see* J.A. 2139
Def't Exh. 6: Spencer McInvaille Report 1464
Def't Exh. 7: Spencer McInvaille Supplemental Report 1469
Def't Exh. 8: CSV Google Data File (.csv file) .....*see* J.A. 2139
Def't Exh. 9: Unique in Crowd Study 1475
Def't Exh. 11: September 2018 Oracle Submission 1480
Def't Exh. 18: Federal Search Warrant Application & Attachments 1502
Def't Exh. 19: State Search Warrants & Attachments 1534
Def't Exh. 21: McGriff Declaration 1 (Doc. 96-1) 1551
Def't Exh. 23: McGriff Declaration 3 (Doc. 147) 1562
Def't Exh. 24: Rodriguez Declaration (Doc. 96-2) 1579
Def't Exh. 27: Every Step You Take 1587
Def't Exh. 30: AZ Ex. 18 (admitted portions only) 1631
Def't Exh. 31: AZ Ex. 19 (admitted portions only) 1633
Def't Exh. 32: AZ Ex. 20 1639
Def't Exh. 33: AZ Ex. 24 1644
Def't Exh. 34: AZ Ex. 202 1667
Def't Exh. 36: AZ Ex. 209 1777
Def't Exh. 38: AZ Ex. 219 1781
Def't Exh. 40: AZ Ex. 236 1797
Def't Exh. 41: AZ Ex. 260 1804

VOLUME 8 (pages 1811 - 2090) – DOCUMENT EXHIBITS, CONT'D

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021), cont'd

Def't Exh. 43: May 2018 Privacy Policy – Redline 1811
Def't Exh. 43a: May 2018 Privacy Policy – Redline (with internet source information) 1840
Def't Exh. 44: Jan. 2019 Privacy Policy – Redline 1865
Def't Exh. 45: Oct. 2019 Privacy Policy – Redline 1895
Def't Exh. 46: McGriff Blog 1 1926

Def't Exh. 47: McGriff Blog 2 1929
Def't Exh. 48: 2018 Quartz Article 1934
Def't Exh. 49: 2018 AP Article 1 1941
Def't Exh. 51: 2019 NYT Article 1948
Def't Exh. 53: Blumenthal-Markey Letter to FTC 1957

Gov't Exh. 1: CAST PowerPoint Presentation 1981
Gov't Exh. 2: Geofence Warrant (Doc. 54-1) ..... *see* J.A. 107
Gov't Exh. 3: Declaration of Marlo McGriff (Mar. 11, 2020)
(same as Def't Exh. 21 (Doc. 96-1)) ..... *see* J.A. 1551
Gov't Exh. 3a: Declaration of Sarah Rodriguez (Mar. 11, 2020)
(same as Def't Exh. 24 (Doc. 96-2)) ..... *see* J.A. 1579
Gov't Exh. 3b: Supplemental Declaration of McGriff (June 17, 2020)
(Doc. 110-1) 2032
Gov't Exh. 3c: Third Declaration of Marlo McGriff (Aug. 7, 2020)
(same as Def't Exh. 23 (Doc. 147)) ..... *see* J.A. 1562
Gov't Exh. 4: Joshua Hylton emails with Google 2034
Gov't Exh. 5: Google Privacy Policy 2048
Gov't Exh. 5a: Google Terms of Service 2081
Gov't Exh. 6: Special Agent D'Errico's C.V. 2088
Gov't Exh. 12: "Got to Be Mobile" Video ..... *see* J.A. 2091

VOLUME 9 (pages 2091 - 2092) – DIGITAL MEDIA EXHIBIT

Gov't Exh. 12: "Got to Be Mobile" Video (admitted only at suppression motion hearing) ..... (.mp4 file)

VOLUME 10 (pages 2093 - 2138) – SEALED DOCUMENT EXHIBIT

Def't Exh. 3: PDF of Raw Data (*see* Doc. 69 (sealing order)) (admitted at both discovery motion hearing and suppression motion hearing) 2093

VOLUME 11 (pages 2139 - end) – SEALED DIGITAL MEDIA EXHIBITS

Def't Exh. 5: Three Paths Video (admitted at both discovery motion hearing and suppression motion hearing) ..... (.mp4 file)
Def't Exh. 8: CSV Google Data File (admitted only at suppression motion hearing) ..... (.csv file, viewable in Excel)

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA	
v.	Criminal No. 3:19CR130
OKELLO T. CHATRIE	January 21, 2020

COMPLETE TRANSCRIPT OF DISCOVERY MOTION
BEFORE THE HONORABLE M. HANNAH LAUCK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

Kenneth R. Simon, Jr., Assistant U.S. Attorney
Peter S. Duffey, Assistant U.S. Attorney
Office of the U.S. Attorney
SunTrust Building
919 East Main Street, Suite 1900
Richmond, Virginia 23219

Counsel for the United States

Laura J. Koenig, Assistant Federal Public Defender
Office of the Federal Public Defender
701 E. Broad Street, Suite 3600
Richmond, Virginia 23219

Michael W. Price, Esquire
National Association of Criminal Defense Lawyers
1660 L Street, NW
12th Floor
Washington, DC 20036

Counsel for the Defendant

DIANE J. DAFFRON, RPR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT

I N D E X

	DIRECT	CROSS	REDIRECT
SPENCER McINVAILLE	17	107	130

E X H I B I T S

		Page
DEFENDANT'S EXHIBITS:		
No. 1	Geofence Warrant and Application	24
No. 2	Google Amicus Brief	26
No. 3	PDF of Raw Data (sealed)	28
No. 4	Activation Video	35
No. 5	Three Paths Video (sealed)	77
No. 6	First Step 2 Request to Google	94
No. 7	Second Step 2 Request to Google	96
No. 8	Third Step 2 Request to Google	97
No. 9	Step 3 Request to Google	100

(The proceedings in this matter commenced at 11:07 a.m.)

THE CLERK: Case No. 3:19CR130, United States of America versus Okello T. Chatrie.

The United States is represented by Kenneth Simon and Peter Duffey. The defendant is represented by Laura Koenig and Michael Price.

Are counsel ready to proceed?

MR. SIMON: The United States is ready, Your Honor.

MS. KOENIG: The defense is ready, Your Honor. Good morning.

THE COURT: Good morning.

MS. KOENIG: Your Honor, we are here on defense motion 28, which is the motion requesting discovery and the subsequent briefing after that.

THE COURT: You're going to have to speak up.

MS. KOENIG: I'm sorry. We are here on defense motion 28, which is the defense motion for discovery and the subsequent briefing after that.

The defense has one witness that we will present to help aid the Court in understanding the materiality aspects of the argument that we make related to the discovery requests. His name is Spencer McInvaille. He already has the proposed

exhibits on the bench. I'm sure the Court should have the proposed exhibits on the bench with all but 4 and 5, which are in the witness folder that we'll seek for admission later.

No. 4 and No. 5 are videos. We had initially thought that we would try to activate a cell phone in the courtroom using a wireless hotspot, and that proved to be a little difficult to try to practice for and enact. So what we did instead is we made visual representations in terms of videos. There are two short videos. And No. 4 is the activation of the cell phone that we will play at the same time we're describing with the witness what is happening.

And then No. 5 is the example -- plotting examples of three individuals whose location data was tracked with the geofence warrant data that Google had provided. In that video itself, there are no location coordinates that are disclosed. It does show a map, like a Google Earth map, with plots being pointed, and next to the plots is a date and time, but it does not have location coordinates.

I think it would be next to impossible for anybody in the audience to decipher any exact locations based on that. So we would proffer that the exhibit could be admitted. I should say it's next to

impossible for anybody sitting in the courtroom here today. I think it would be relatively easy for anybody who has unfettered access to that exhibit to figure out the location coordinates. And so we have a proposal, but if the Court would like us to have the entire exhibit published and submitted under seal, we can do that. But I do think that it could be published publicly here in the courtroom, but it would need to be under seal for all the reasons that we had submitted in ECF No. 68, and that the Court had ordered sealed in ECF 69, based on the raw data, because those plots are based on the raw data.

The only other issue before the Court is that both parties have agreed to ask the Court to cross-designate their experts as advisory witnesses. Ours, as I mentioned before, is Spencer McInvaille, and the government may call, in response to Mr. McInvaille, Jeremy D'Errico. And we have no objection, and they have no objection to either being cross-designated as advisory witnesses.

THE COURT: All right. Well, let me ask you first, do you or the government have a position as to whether or not the rules of evidence pertain to this hearing?

MS. KOENIG: I think that the rules of

evidence apply, but because this is relating to the admission of evidence, I think we're seeking -- I guess the purpose of this hearing is for the Court to order whether or not evidence will be disclosed. And so that relates to the admissibility of evidence, which under the rules of evidence operates under a relaxed standard. And so I don't think that, specifically, like hearsay rules would apply. I don't anticipate that that's going to be too much of a problem at this hearing.

THE COURT: All right. I'm going to ask the government to speak, please.

MS. KOENIG: Thank you, Your Honor.

THE COURT: So, first, Mr. Simon, I'd like to ask you to take a position on the defense's proposed course of action, whether you have any objection or different proposal, and I also want you to address whether you think the rules of evidence apply.

MR. SIMON: Judge, no objection to the use of the raw data in this courtroom or the cross-designation of the witnesses as advisory witnesses. And Special Agent D'Errico, we'll bring him in during the testimony of Mr. McInvaille.

With respect to, Judge, the Federal Rules of Evidence, we do believe they apply here, and I think

it brings into sort of the picture here a bigger question, which is whether, at this stage, whether in a motion for discovery hearing we're moving toward where we will be for a suppression hearing in February in terms of some of the testimony that I think will be gleaned here. We'll certainly listen to it, but there may be a relevance objection to a number of the -- some of the testimony elicited here.

I think with respect to the Federal Rules of Evidence, they should apply. And to the extent that they --

THE COURT: Do the rules of evidence apply in a motion to suppress?

MR. SIMON: Yes, Your Honor, I think the rules of evidence would apply here.

THE COURT: In the motion to suppress.

MR. SIMON: In the motion to suppress hearing, yes, Judge.

THE COURT: Well, what do I do, first of all, with the fact that you all disagree about what rules I should be applying?

MS. KOENIG: Your Honor, I'm looking at Federal Rule of Evidence 1101(d)(3), which says that these rules, except for those on privilege, do not apply to the following, and it says "miscellaneous

proceedings such as." And then jumping to the portion that would be applicable here, "The preliminary examination in a criminal case" -- I'm sorry. Not that. But (c) -- I'm sorry. (d)(1), which is the Court's determination under Rule 104(a) on a preliminary question of fact governing admissibility. But this is also a miscellaneous proceeding under (d)(3).

I think under either one of those the Court is looking at evidence in this case in a very preliminary matter, not in terms of finality of what would be presented at a trial or what would be presented in something where a final judgment would be rendered. And so based on those exceptions to when the rules of evidence apply, I think they don't apply, but even if they did apply in some fashion, it would be a very relaxed standard as in the motions to suppress.

THE COURT: Explain to me your position on the standard in the motion to suppress.

MS. KOENIG: Your Honor, and I apologize. I don't have the case in front of me, but I think there is case law from the Fourth Circuit which indicates that in a motion to suppress, because it is governing the admissibility of evidence, that to the extent that

rules of evidence are adhered to in any motion to suppress, they are under a very relaxed standard. I'm sorry I don't have the case cite, Your Honor.

THE COURT: That's fine.

MR. SIMON: Judge, I'll agree with that. I think the -- I was incorrect to the extent that I indicated that they would apply. And certainly to the extent they would, it would be a relaxed standard in terms of the suppression hearing. And here, the bigger point there, Judge, is just with respect to the testimony elicited and its potential relevance here to the motion for discovery. And I think we can get to that point based off of the testimony that they will elicit.

I think it would be helpful, Judge, to kind of note, and maybe for defense counsel, to the extent that they disagree, to put on the record where I think there is agreement at this point with respect to the motion for discovery, which paragraphs have been addressed sufficiently, which are still in dispute, and which relate purely to documents that might be in the possession of Google to the government's viewpoint.

THE COURT: Well, why don't you all discuss that together and see if you can put that on the

record in a stipulated fashion.

MR. SIMON: Okay. And, Judge, I'm happy to say it right now before the Court, and to the extent that defense counsel disagrees, I think some of this has already been put on the record. I just wanted to be clear before testimony was elicited about some of the paragraphs here. So in --

THE COURT: Just a minute. Let me catch up with you.

All right.

MR. SIMON: And so in ECF 28, this is the discovery motion, first, to note which have -- the parties agree have been made sufficiently and where that can be found. Paragraph 6 with relation to the physical access to any and all devices and software, to the extent that that would be provided, the defense agrees on page 1 of their reply that that is sufficient at this stage for their warrant. Same with paragraph 7, copies of the raw data produced and utilized by law enforcement. I think both parties now, obviously, recognize that that's been produced, and I think that's made clear on page 1.

The reply of the defendant, as well as paragraphs 11(a) and (b), that relates to communications concerning the geofence request in this

case, communications with Google, as well as any arrests and investigative reports. I don't believe there were any as it related to that, but to the extent that there were, they were turned over. And so there's agreement as to those three paragraphs.

There could potentially be additional disagreement about paragraph 2 and paragraph 8. So paragraph 2 is the anonymous identifier as it relates to Mr. Chatrie's -- pardon me -- anonymous identifiers provided by Google and its returns. The United States has made clear that that was provided and gave the last four digits of that as it's laid out in the raw returns from Google. It just seems that the defendant was unable to ascertain which account was his, but that number is in the raw data return in paragraph 2. So I believe we agree at this point that they have the anonymous identifier that relates to Mr. Chatrie.

And then for paragraph 8, all information about how law enforcement officials manipulate and analyzed the data in this case to identify the second and third rounds of the search process, there's no documented record of that in terms -- that would be turned over by a *Jencks*, or if there was some other sort of documented piece of that. There will be witness testimony to that point, and certainly to the

extent that it's involved in expert notice, we provided there. But I don't think that there's anything discoverable at this point, documentary evidence as to paragraph 8. Purely, there would be witness testimony. To the extent that our expert was involved in that, it would be certainly provided in the expert notice that the Court has ordered produced on February 3rd, to the extent that that comes.

With relation to paragraph (c), (d), and (e) of paragraph 11, it continues to be the position of the United States that to the special agent who's tasked with or who has a knowledge of those kinds of documents, they are not available. They do not exist. And, again, to the extent that that were to change, we'd provide those documents to the defense.

The remaining paragraphs, paragraphs 1, 3, 4, 5, 9, 10, all relate to documents that we have argued and continue to argue are in the possession, custody, and control of Google for purposes of Rule 16, and to the extent that there would be some sort of *Brady* requirement, Google is not a part of the United States' investigative team in terms of those documents. But, again, we produced everything that Google has provided to us. And so I think that is an accurate and fair lay of the land, but to the extent

that there's some disagreement there, I think defense counsel can inform the Court.

THE COURT: All right. So, I'm just going to make the finding so it's clear on the record that for purposes of this hearing with respect to the rules of evidence, I do think under Rule 1101(d), it is appropriate to apply the relaxed standard similar to that undertaken in a motion to suppress. It certainly makes no sense that it would be harsher than a motion to suppress, and it's quite possible that under some of the provisions in (d)(1), they may not apply at all, but we will address each issue as it comes up.

So I'll hear from the defense as to what is or is not in dispute.

MS. KOENIG: Your Honor, as it relates to paragraph 6 and 7 of document No. 28, we will agree that those have been provided sufficiently and satisfactorily.

As it relates to paragraph 2, which is the anonymous identifier, we still don't have any formal recognition of which identifier is Mr. Chatrie's. I think we have a good idea, but I don't want to foreclose that until we have witness testimony.

Paragraphs eight and eleven, we do anticipate presenting evidence as to why we need those requests

satisfied.

And then, as Mr. Simon indicated, the remaining paragraphs 1, 3, 4, 5, 9, and 10, we will lay a foundation as to why those are material, and then we'll get into the legal arguments about how that applies at this hearing.

THE COURT: All right.

MS. KOENIG: Thank you, Your Honor.

THE COURT: Mr. Simon, I'm sorry to make you bounce up and down, but the defense has provided a witness list and exhibit list. Do you have one?

MR. SIMON: Yes, Judge. I received it this morning.

THE COURT: No. Do you have one for me?

MR. SIMON: No, we do not have an exhibit list, in part because we're not certain we'll call Special Agent D'Errico, and so there's no formal exhibit list.

THE COURT: And no witness list?

MR. SIMON: No witness list, that's right, Judge.

THE COURT: Okay. Thank you.

All right. We can begin the process. And with respect to the pieces of evidence and the video or the ones that are under seal, I am inclined to have

this evidence on the record under seal rather than just having it viewed during the hearing itself. So I grant the motion to seal and place it in the evidentiary record. Does anybody object to that?

MR. SIMON: No objection, Your Honor.

MS. KOENIG: No objection.

THE COURT: All right. I want to be clear that I think for purposes -- I've read your briefing, and I understand that this is meant to elucidate to me the importance of what is or is not discoverable.

I want to be clear that both parties have to be exacting in whether they are talking to me about the Rule 16 standard or the *Brady* standard because they are not the same. And I want the arguments not to blend those standards because it's not helpful to the Court. Specifically, with respect to materiality, it's not the same test.

I also want you all to keep in mind that there is -- I want you to educate me about how I apply these standards. And the specific issue being that the *Brady* standard for materiality is whether it's a reasonable probability that had the evidence been disclosed to the defendant, the result of the proceeding would have been different. Under Rule 16, "materiality" is defined as some indication that the

pretrial disclosure of the evidence would have enabled the defendant to significantly alter the quantum of proof in his or her favor.

Now, obviously, these are both backward-looking tests, and so I want you to educate me about how I apply them forward-looking, because we don't have an outcome. And so I just want you all to be mindful of that as well.

I also need, at some point, for the defense to address the 17(c) argument raised by the United States. It is not addressed at all in briefing, and I think it's relevant, and so that's got to be addressed also.

So those are my preliminary comments.

MS. KOENIG: Your Honor, the defense first calls Spencer McInvaille.

THE COURT: Is there a witness exclusion motion?

MS. KOENIG: Your Honor, if the Court will order that we can cross-designate Mr. McInvaille and Mr. D'Errico as advisory witnesses, we don't need an order of sequestration because there would be no order witnesses presented.

THE COURT: All right. Agreed?

MR. SIMON: No objection to that, Your Honor.

THE COURT: All right. Okay. We'll move forward.

SPENCER MCINVAILLE, called by the Defendant, first being duly sworn, testified as follows:

MR. PRICE: Good morning, Your Honor.

THE COURT: Good morning. Can you place your name on the record?

MR. PRICE: Sorry. Michael Price with the NACDL Fourth Amendment Center for Mr. Chatrie.

DIRECT EXAMINATION

BY MR. PRICE:

Q Good morning, Mr. McInvaille.

A Good morning.

Q Could you please state your full name for the record?

A Spencer McInvaille.

Q Where do you currently work?

THE COURT: Can you spell it, please?

THE WITNESS: Yes, ma'am. It's M-c-I-N-V-A-I-L-L-E.

THE COURT: Thank you.

A I currently work for Envista Forensics. That's

E-N-V-I-S-T-A.

Q What do you do at Envista Forensics?

A I am a digital forensics examiner.

Q What does that entail, generally?

A I deal with various types of location data, cell phone forensics, records from phone carriers, various types of location information, GPS, several different forms.

Q Prior to working at Envista, were you employed?

A Yes. I was a law enforcement officer in Lancaster, South Carolina.

Q What did you do as a law enforcement officer in South Carolina?

A I was a violent crimes investigator. Part of my task was also on the Internet, Crimes Against Children Task Force, as well as mobile phone forensics, and location data examination.

Q Could you expand on that a little bit more? You used location data for what?

A Location data for various things. So investigations of various violent crimes. Also similar types of data for investigations of child exploitation, as well as locating fugitives from our county.

Q Thank you. Do you have any certifications that

are relevant?
A Yes. I hold certifications from Cellebrite for mobile phones forensics, as well as certifications for telecommunications. So dealing with the different networks that we see.
Q Have you had any training dealing with location data and interpreting location data?
A Yes, training in GPS, call detail records, historical records. I believe I mentioned GPS, and then various types of information that we get from Google and various places.
Q Do you recall how many hours of training you might have had?
A Quite a few. Several different classes.
Q Have you been qualified as an expert before?
A I have.
Q How many times?
A I believe 11 times.
Q Do you know what a geofence warrant is?
A Yes.
THE COURT: An expert in what?
MR. PRICE: Sorry.
BY MR. PRICE:
Q You've been qualified as an expert before 11 times. How have you been qualified?

A In mobile phone forensics as well as historical cell site analysis.

THE COURT: And who were the trainings with?

THE WITNESS: Cellebrite, as well as Terracom, and my company as well.

THE COURT: Thank you.

BY MR. PRICE:

Q So, we'll get into the details in a minute. I just want to ask you, generally speaking, do you know what a geofence warrant is?

A Yes.

Q Generally speaking, how does a geofence warrant operate?

A A Geofence request to Google is a request based on an incident occurring, determine that incident's location, and its date and time, and drawing some sort of boundary around that area that you would like searched. That request goes to Google for them to then search the users that could have been in that area at that time and then return that information for it to be analyzed.

Q Is that an iterative process?

A Sir?

Q Does that process take place in more than one step?

A Yes, it does take several steps.
Q How is that different from the usual way that you have seen location data produced?
THE COURT: You're going to have to pull up the microphone a little bit, because you're looking more at him than you are into the microphone. And it's hard for me to hear and I'm sure my court reporter, too.
BY MR. PRICE:
Q The location data in this case, how is that different from location data that you have seen in other cases?
A So, typically, when we're dealing with like historical cell cite information, different requests from Google, those requests are made based on individual users. So we know a certain account or a phone number that we're looking for, and we make a request to the correct company to get those records.
Q Thank you. Have you received any formal training or in-class training on geofence warrants?
A No, sir.
Q Why not?
A That is not available to non-law enforcement.
Q What materials have you reviewed that are related to the geofence warrant in this case?

A We have the returns from Google, the amicus brief from Google, the emails and correspondence between the detective and Google. I believe that's it.
Q Anything else? The warrant?
A Oh, as well as the search warrant. Excuse me.
Q What sort of experience do you have with Google's public-facing policies, their privacy policy?
A Just what you can find available on their website.
Q What is your past experience with Google's location data production? Is this typical?
A I have seen both geofence responses as well as account-specific responses.

MR. PRICE: Your Honor, at this time I'd like to tender Mr. McInvaille as an expert in the field of digital forensic examinations, mobile forensics, and cellular location analysis.

THE COURT: No objection, correct?

MR. SIMON: No objection, Your Honor.

THE COURT: He will be deemed an expert.

MR. PRICE: Thank you, Your Honor.

BY MR. PRICE:
Q I'd like to ask you some questions now specifically about Google and what Google provided to law enforcement in this case. How does Google say it categorizes different types of location data it

obtains?
A As far as Google, they classify them differently. They have Google location services, your web and app activity, as well as Google location history.
Q And can you tell us briefly what each one of those is? What is Google location services, generally speaking?
A So, Google location services is a service through Google that uses their various systems through your device to locate you so that you can navigate around town, find restaurants, all of the conveniences that we find in our devices.
Q And what about web and app activity?
A So web and app activity also track similar items. So searches, the things that you do within your apps. Those items are used and tracked across platforms with Google to, again, enhance the user's experience.
Q And then there's a third category, location history. What is that, generally?
A So, location history is essentially a kind of gathering of those pieces of information stored so that your device and your account can better aid you in finding relevant locations that you would want to use, as well as being able to keep the data that you generate.

Q Thank you. I want to ask you to turn to what's been marked as Exhibit 1 in your folder there. Do you recognize the document?
A Yes, affidavit for a search warrant.
Q And is that the search warrant you reviewed in this case?
A Correct.
MR. PRICE: I'd like to introduce that into evidence as Exhibit 1.
THE COURT: Any objection?
MR. SIMON: No objection, Your Honor.
THE COURT: It's entered.
(Defendant's Exhibit 1 is admitted into evidence.)
BY MR. PRICE:
Q Could you read the first bullet point, page 2? I'm sorry, the second bullet point, the first full sentence beginning with "for each type."
A I'm sorry. I'm not picking up where you're at.
Q It's marked page 2. It's actually page 4 of the PDF.
A Gotcha. So, the second bullet point?
Q The second bullet, first sentence, please.
A "For each type of Google account that is associated" --

THE COURT: Sir, it's human nature, if you're reading something, to speed up, but our court reporter needs to get every word. So just read it as if you were saying it, not as if you are reading it. It happens all the time.

A I understand. That's all right.

"For each type of Google account that is associated with a device that is inside the geographical area described further and attachment to during the time frame listed above, Google will provide anonymized information regarding the accounts that are associated with a device that was inside the described geographical area during the time frame described above. The anonymized information will include numerical identifier for the account, the type of account, time stamp location coordinates, and the data source that information came from, if available. The information initially provided by Google will not contain any further content or information identifying the user of a particular device or account."

Q I just want to call your attention to the first sentence there. It says "for each type." So what types of location information did this warrant ask Google to produce?

A Each, all, is what it appears to be.

Q What would that mean to you? "Each" meaning?
A Anything that Google retains as far as accounts with location that they can search.
Q Would that include the three types of location data that we just talked about?
A Correct.
Q I want to ask you to turn to Exhibit 2 in your folder there. Do you recognize that document?
A Yes, the Google amicus brief.
Q And that's the brief that you reviewed in this case?
A Correct.

MR. PRICE: Your Honor, this is already a part of the record, ECF No. 59-1. We don't seek to introduce it as evidence here but just to mark it as Exhibit 2 for purposes of this hearing.

THE COURT: All right. It will be marked. No objection, correct?

MR. SIMON: No objection, Your Honor.

(Defendant's Exhibit No. 2 is marked for identification purposes.)

BY MR. PRICE:
Q Would you turn to page 12 of that document for me and read the last sentence of the first full paragraph in parenthesis?

A "In order to comply with the" --
Q It begins with "in practice."
A Excuse me.
Q The last sentence of the first full paragraph.
A The first full paragraph. Excuse me. "In practice, although the legal requests do not necessarily reflect this limitation, such requests can cover only Google users who had location or LH, location history, enabled and were using it at the time in question."
Q Just so we're clear, what does LH stand for?
A Location history.
Q Okay. And so what is Google saying there?
A It's saying the request can only cover Google users who had location history enabled.
Q So they're saying they only produced one of the three categories?
A Correct.
Q All right. I want you to turn now to what's marked as Exhibit 3 in your folder.

MR. PRICE: And this, Your Honor, should be published only to the Court. It's under seal.

THE COURT: All right. So that will be published just to the Court and the parties under seal.

BY MR. PRICE:

Q Do you recognize the document?

A Yes.

Q What is it?

A It is the Google returns from Google, the returns.

Q And these are the raw data returns that you reviewed in this case?

A Correct.

MR. PRICE: Your Honor, these are marked as Exhibit A attached to document 68. We would like to mark them as Exhibit 3 here.

THE COURT: All right.

MR. SIMON: No objection.

THE COURT: Thank you. They will be marked as Exhibit 3 and entered under seal.

(Defendant's Exhibit No. 3 is marked and entered under seal.)

BY MR. PRICE:

Q So tell us what you see at the beginning of the raw data provided here. What types of location data did Google produce?

THE COURT: You're going to have to direct the Court as to what page you're looking at, at least. Somehow identify it.

MR. PRICE: Excuse me, Your Honor. It's page

6 of the PDF itself. I don't believe they have page numbers. It's the first page with data on it.

A So, this is the location history for various device IDs.

BY MR. PRICE:

Q How do you know that it's location history?

A It has locations, and this is what we typically get in return.

Q Does it indicate the source of the data here?

A It indicates what the measurement was taken from, as far as Wi-Fi or GPS.

Q Does it say whether it was data obtained from Google location services or web and app activity or location history?

A It does not.

Q So it doesn't say what type of -- as far as Google is concerned, not GPS or Wi-Fi, but the types of categories of data that we talked about before, it doesn't indicate that here?

A Correct. It doesn't specify the Google category that this falls into.

Q Why?

A I'm not sure.

Q How is that different from Google location data produced to you in other contexts that you've worked

on before?
A So, typically, if you were to see a return for a specific account, for one, the document is named by the user's account name as well as the user name, location history, and then the file type.
Q So it would indicate location history, for example, if it was produced from location history data?
A That's correct.
Q Do you know why Google doesn't do that here?
A I'm not sure.
THE COURT: Wait. When you say "typically," what do you mean? Typically, when you're just looking at a known account or typically when you're not looking at a known account?
THE WITNESS: When you are looking at account-specific requests, that's how it is shown.
THE COURT: Okay.
BY MR. PRICE:
Q So Google didn't indicate location history, but they said they did only location history. Do you know why they would have produced only location history data?
A No, I do not know.
Q Do you know why they wouldn't have produced web

and app activity data?
A I don't.
Q Do you know why they wouldn't have produced Google location services data?
A I'm not sure.
Q Why don't you know?
A There's not an explanation of why.
Q Would --
THE COURT: Not an explanation of why on the document, is that what you mean?
THE WITNESS: Correct, in any of the documents provided.
THE COURT: All right.
BY MR. PRICE:
Q Would Google have policies and procedures about this?
A I'm sure they would.
Q Why do you think so?
A Clearly, something guided them to provide a certain data or search a certain set of data.
Q Have you seen those policies or procedures?
A I have not.
Q What do you think they might tell you if you were to see them?
A I'm sure they would outline the process that

Google has outlined for their analysts who provide data in response to a legal process request.

Q Is that information in the warrant or application?

A The information -- I'm sorry?

Q Is that information in the warrant or application?

A The request?

Q The information that you might learn from looking at the policies and procedures.

A I don't see it in the search warrant, no.

Q And it hasn't been provided to you in any way?

A No, sir.

Q I'd like to talk a little bit now about location history specifically and what's involved in enabling it. In the amicus brief that you reviewed, Exhibit 2 that we've already talked about, Google says that this sort of trademarking is entirely voluntary, citing six steps. Can you tell us what those six steps are on page 8?

THE COURT: Are we back to --

MR. PRICE: We're back to Exhibit 2, Your Honor.

THE COURT: -- Exhibit 2?

MR. PRICE: Yes, Your Honor.

BY MR. PRICE:

Q The bottom of page 8.

A I'm sorry. I'm not seeing it on 8.

THE COURT: The paragraph starts, "The user thus controls her Google location history data, which is LH, unlike, for instance, the CSLI at issue in the *Carpenter* case that the parties have referenced for cellular data."

MR. PRICE: Excuse me, Your Honor. It's my fault. It's the first paragraph on page eight. And it starts on page 7, the last sentence. "Specifically, the user must opt into."

THE COURT: Okay. Make this clear. What do you want him to read from so I can follow you, please?

MR. PRICE: The paragraph starting on page 7 beginning with "specifically."

THE COURT: So it's the middle of the --

MR. PRICE: The last sentence on page 7 going into page 8.

THE COURT: Are you with us, sir?

THE WITNESS: I am.

THE COURT: All right.

A "Specifically, the user must opt into location history in her account settings and enable "Location Reporting," a subsetting within location history, for the particular device. And to actually record and save location history, the user must then sign into

her Google account on her device and travel with that device."

BY MR. PRICE:

Q So Google is saying that this is a fairly deliberative process. Do you agree that enabling location history requires such deliberate choices?

A Yes and no.

Q Can you explain a little more?

A So you do have to make the selection to activate location history. The method in which that typically happens and the way that you see it on the device is through prompts that tell you not that location history needs to be enabled, but that if you opt into certain functions, that it does improve your experience. You do not receive the type of information that would lead you to believe that what you have here contained in location history and what it can be used for is exactly what you're opting into.

Q So did you prepare a demonstration to illustrate this point?

A Correct.

Q All right. Let's talk about what you did. You made a visual presentation of the setup process?

A I did.

Q For an Android phone?

A I did.
Q And the visual presentation is in the form of a video?
A It is.
Q That's 4 minutes and 46 seconds long?
A Yes.
Q And you have that video on a DVD in front of you marked Exhibit 4?
A I do.
Q And you have reviewed that DVD prior to coming to court today and have verified it's the same video you created?
A I have.
Q You marked the DVD with your initials reflecting that?
A I did.
Q All right.

MR. PRICE: Your Honor, I'd like to move to introduce the video as Exhibit 4 and publish it.

THE COURT: Any objection?

MR. SIMON: No objection, Your Honor.

THE COURT: All right. It will be entered.

(Defendant's Exhibit No. 4 is admitted into evidence.)

BY MR. PRICE:

Q Before we get started with this video, I want to ask you a couple of preliminary questions. Is this the same phone that the defendant -- at issue here with the defendant?
A It is not.
Q Why is it not the same phone?
A This is a test device that we have at Envista.
Q Okay. Is it running the same operating system?
A It is an Android operating system.
Q Is it running the same version as the defendant's phone?
A This is running Android 7.
Q So it's one version earlier?
A It is. Android 8, I believe, was the defendant's phone.
Q Have you had an opportunity to compare version 7 and version 8?
A I haven't device to device, but I was able to review articles and literature that I could find between comparing the two, and they're very similar.
Q How did you make that determination?
A In comparison to what I've seen here as well as the various screenshots and things that I was able to find for that setup.
Q So just to be clear, the screenshots for version 8

are the same as version 7, to your knowledge?

A They're very similar, yes.

Q All right. So, let's go through this video. Can you talk us through the steps here on what you've done?

A Absolutely. So, when you first boot the phone up, this is the welcome screen that you would get prior to a phone being set up. So similar to it coming straight out of the box after you purchased it. So you will begin the process.

In this first screen, which is labeled "input method," you're going to --

THE COURT: So, listen. I'm going to ask you all to be very careful about establishing the record. If you're switching the screens you're looking at, you have to stop and be clear the first one is the start-up. Give us a moment to keep up with you. This is the second screen that pops up.

THE WITNESS: Yes, ma'am.

THE COURT: It does pop up or however you access it. So we need to slow down so I can follow you, because I haven't seen this before, and it's helpful for me to be able to be sure I'm absorbing what you're saying.

THE WITNESS: Understood.

A This is the second screen. This is the input method. So we're choosing what type of keyboard and icons that you would see in the -- through the process of setting up the device and then later that you will see in the device.

So here we're going to select that we would like the English keyboard, and we're going to move to the third screen.

Here we have to establish on the third screen an Internet connection so that we can complete the process. So here you will see several steps to complete that process.

Moving to the next screen where we will select the Wi-Fi access point to use to complete the setup.

So we enter the password here for that access point so that we can establish a connection.

THE COURT: To be clear, a pop-up came up prompting the entry of the password.

THE WITNESS: That's right.

A And after that's entered, we will be connected and move to the next screen. In this next screen, we have the terms and conditions for the device itself from its manufacturer. We will see several different terms and conditions, but this is the first relating to the manufacturer of the device.

BY MR. PRICE:

Q Before you go through that, or when you're going through that, can you tell us if that mentions location history or mentions Google, specifically?

A It does not.

So after scrolling through those items and clicking to the next button, you're prompted to either agree or disagree with the terms of service for the device.

THE COURT: Can I ask you a question? Did you go all the way through? How many terms and conditions are there?

THE WITNESS: There are six. That's the extent of them there.

A So now we'll move to the next screen, and it will check the connection for the device and take a moment before it moves to the next screen where we have to make indications or selections on the device.

BY MR. PRICE:

Q While we're doing this, I just want to be clear. The privacy policy for the phone itself, the ASUS policy, can you explain what, if any, relationship that has to Google?

A I did not see a direct relation or mention of Google in that setup.

So, we're finally to the next screen. On this screen it's asking if we have another device to use to set up this new device. So this would be if you want to transfer data and settings from one device to this new device that you're accepting up. Here, since I'm setting this up for the purposes of this and not trying to retain any previous data, I'm going to select "no thanks" and move on to the next selection.

So, again, it's going to run through checking the device for various things that it needs to complete for setup, and we'll move on to the next indication when available.

So, for Android devices to complete the kind of user experience and use all of the functions of the device, Android would like for you to activate or connect a Gmail account to the device itself. So here you can either enter in an existing account or create a new account.

For the purposes of this, we're going to create a new account. After that selection, it will move to a new screen. And on that new screen we will enter a name and some various other information so that we can begin to complete the account creation.

We're moving to the next screen.

THE COURT: I'm going to interrupt you a

little bit. You said the Android would like you to activate through a Gmail account. Is there an option not to?

THE WITNESS: You can skip that function.

BY MR. PRICE:

Q May I follow up on that?

A Yes.

Q What's the consequence of skipping that function?

A You lose much of the functionality of the device where you would go download applications from the app store and many of the other functions --

THE COURT: Are you getting to that later?

THE WITNESS: We did not skip that process. We're setting this phone up as if --

THE COURT: Are you going to testify about how that happens later?

THE WITNESS: About how --

THE COURT: If you don't use Google, what happens?

THE WITNESS: Correct. We can discuss that.

Q Please. So if we don't have --

THE COURT: Go back to the Android account, the screen before. So the person's index finger is covering the word "skip."

THE WITNESS: Correct.

THE COURT: On the screen, it says you can skip it.

THE WITNESS: Yes.

THE COURT: All right.

BY MR. PRICE:

Q In your experience, have you ever received a pop-up message when hitting skip?

A Yes. It does ask you are you sure you want to not set up an account on the device.

Q And it describes some of the features that you might be missing out on; is that correct?

A I do believe so.

THE COURT: Wait. I'm sorry. I got -- say that again, please.

THE WITNESS: That's all right. If you skip the function, it does ask you are you sure you want to skip this function as it may hinder you from being able to use the device to its fullest extent.

THE COURT: All right. What happens if you say you're sure?

THE WITNESS: Then you don't set up an account on that device, and then you aren't able to access things like the application store and other functions of the device that we would all normally use.

BY MR. PRICE:

Q Would you be able to use any Google service at all?

A I still do believe you would be able to use some of the functions of the device.

Q But the Google services in particular without an account?

A I do not believe you would be able to use like Google location services, and things like that, that help with your map functions. Location as a whole in the device would still be available, but many of the Google-related functions would not be available.

Q Like maps?

A Correct.

THE COURT: Anything else? I'm looking for specifics here.

BY MR. PRICE:

Q What about email?

A You would not have your Gmail account attached. There again, you wouldn't be able to access the app store, which is where you --

Q Can you explain what that is?

A Yes. That's where you download the various applications that you would use. So if you wanted to add your bank application or various other

applications that people typically use, you wouldn't have that functionality.

Q So you'd be left with what on the phone? What it came with?

A Essentially, yes.

Q And you wouldn't be able to install any apps from the app store?

A Correct.

Q Or use any of the Google app services?

A Correct.

THE COURT: I'm going to interrupt you again. I'm not an expert in this.

THE WITNESS: That's all right.

THE COURT: So, first off, I know we're talking about an Android because there's an Android at issue. Would this testimony be different under Apple?

THE WITNESS: Yes, it can be.

THE COURT: Do you know whether or not if you don't sign up with a Google account in Apple -- first of all, does it ask you to do that?

THE WITNESS: What? In Apple? No, I think Apple would probably prefer that you didn't use Google services. I think they would prefer that you use theirs.

THE COURT: Just making it clear.

THE WITNESS: But you can add Google services to your iPhone.

THE COURT: All right. And I want to be clear about -- you testified earlier about the system. So, this is an Android phone.

THE WITNESS: Yes, ma'am.

THE COURT: And is this the same kind of phone that Mr. Chatrie is alleged to have carried?

THE WITNESS: No, it's not the same device.

THE COURT: Why are they comparable?

THE WITNESS: They are running Android software.

THE COURT: Okay.

MR. PRICE: Perhaps I can ask a few questions to clarify, Your Honor.

THE COURT: All right.

BY MR. PRICE:

Q The current version or the phone that the defendant had was the Samsung S9; correct?

A Correct.

Q Did you purchase an S9?

A We did.

Q When you go through this process, what operating system does it load up?

A It loads with Android 9.

Q Is Android 9 significantly different from Android 8?
A It seemed to be. Between 7, 8, and 9, 9 seemed to be much more different than the comparison of 7 to 8.
Q And with 9, again, which is not at issue here, did you find that some of the information about location services was different?
A It does. It prompts differently, but you still end up with the same prompts for location services and location history.
Q Would a normal user who purchases an S9 today be able to downgrade and load the previous operating system through the normal process of setting up the phone?
A Not through the normal process. It's -- I mean, it's not terribly complicated, but it's not something that you would typically see from the average user.
Q You had to download special software from the Internet to even give this a try; is that correct?
A Yes. You would have to download the old firmware version and load it to the device.
Q When you attempted to do that and reboot the phone, what happened to the operating system you installed?
A On that device when you provide it with the old

software, it still wants to, without a connection or with a connection, still pushes towards that Android 9 interface and its functionality.

Q So, would it be fair to say that one of the reasons we used a different phone and a different operating system here is because it is the most comparable to the system and the phone at issue in this case?

A Between what I worked on, yes, it was more comparable.

THE COURT: And there's no material differences between the terms and conditions of this example and what Mr. Chatrie is alleged to have had?

THE WITNESS: That would be hard to speak to just because how often Google can change the terms. So at the time, across platforms, the terms would be the same as they come from Google, and through that Internet connection is where you're receiving those. So they seem to be, across platforms, the exact same terms and policies that come from Google. Most are dated with their release time.

THE COURT: Okay.

BY MR. PRICE:

Q You said -- you mentioned seeing articles that describe the setup process in version 8. Did those

have images of the setup process?
A They did.
Q Were they the same as the ones in version 7?
A Yes, they looked very similar.
Q Were both of those different than the information about location history provided in operating system 9?
A The materials are the same. It doesn't look different, but it's the same request and prompt from Google.
Q Thank you.
MR. PRICE: Your Honor, do you have any more questions before we proceed?
THE COURT: No. Thank you.
MR. PRICE: Okay.
A So we're going to go back into the setup process here. We're just creating the account by providing a name. After you provide the name, it will move on to the next selection.
On the next screen, it provides -- it wants you to provide a date of birth. That's typically for the play store so you can determine what you're going to download if it's appropriate.
THE COURT: Just to be clear, that screen was entitled "Google Basic Information."
THE WITNESS: Correct.

A And after that selection has been made, it moves to the next screen, which is "choose your Gmail address." It provides two selections that it created as well as a selection where you can create your own. I just opted to use one of the already generated addresses.

And it moves to the next screen where we'll now input -- and it prompts you to create a password for your account.

BY MR. PRICE:

Q In your expert opinion, is password 1-2-3 a strong password?

A It's a terrible password.

After you enter your password and confirm it, it will now prompt you to the next screen.

This next screen would like you to add a phone number to the account. It explains that there are several different reasons you would use this; to reset your account, receive messages, as well as make Google services relevant to you. And there's a scroll down here to add other -- to kind of further explain some of those -- what can be used and how you can use it.

Q To be clear, does this mention location history?

A It does not. And you can either skip, you can say yes, I'm in, and add a phone number, and then there's

also a "more options" selection. So I'm going to select "more options" here.

So it just takes you to the screen to give you the three different choices that you have here. You can not add your phone number, you can add your phone number with all of the features, or you can add your phone number only for security reasons. I did not add a phone number and moved on to the next screen.

Here it's going to show you your account name, your name, and you can select "next" to continue with the process.

THE COURT: The title of that screen is "Review Your Account Info," the new screen.

THE WITNESS: On the next screen after moving on, this is Google privacy and terms. Here is where it explains out and has all of the links to the various websites or web addresses within Google where you can read all of the terms and conditions for various -- the account itself, for like Google Play as well as the privacy policy.

This goes down quite a -- it has quite a bit of information contained within it as well as several links to Google's website with pages upon pages of information about their privacy policy.

BY MR. PRICE:

Q Just to be clear, does this screen say anything about location history?

A It doesn't yet. There is various information down this screen. You can still choose not to create the profile that you have begun to create. You can simply agree now and move on or you can select "more options."

Under "more options," we now get into some of the information that we spoke about earlier that Google has as far as their services, starting here with web and app activity.

Q Is there a default setting for that?

A The default setting for web and app activity there is the affirmative already. So it would be for you to deselect that if you didn't want that selection within the Google services.

The next being "add personalization." It is, as well, in the affirmative selection. It, again, would be up to you to deselect.

"YouTube history," the same. It is in the affirmative to save your Google or your YouTube history into your Google account.

And then, finally, "Google location history" being the final selection on this page. Out of that group, it is the only one that is not currently selected. It

would be up to you to opt into the Google location history at this time.

Once you get down to the bottom again, you still have the choice to not create the account or you can agree and move on with the account.

I'm going to press "agree," and move to the next screen. Again, it's checking the device. "Checking info" is what it displays, and you have to wait until the next prompt.

The next prompt is labeled "Google Services." It says you can turn on or off any service for the following account. And then it goes through and advises the different services, again, that you can turn on or off.

You'll see "automatically backup data" is in the affirmative position. "Google location services," again, affirmative. "Improve location accuracy," it is also selected. And "improve your Android experience," it is also selected.

"Keep me up to date," meaning receive emails about Google, is in the affirmative. And then if you agree, you can move to the next or deselect any of those.

It's going to ask to set up payment information on the next screen. You can choose to set it up or not. We said "no thanks" and continued. Again, checking

the device and waiting for the next prompt.

The next is for you to confirm the date and time for the device to be used, and we will select "next."

And then to this next screen it is "protect your phone." This is where you would enable a pass code or some kind of lock on the device to protect the device.

Q May I pause here, Spencer?

A Yes.

Q Sorry. Mr. McInvaille.

Prior to this step where you're setting up the pass code, can you tell us which of the three categories of location history have been enabled by default?

A So no location history has been activated, but location services and Google location services, as well as web and app activity are selected at this point.

Q And a user who's going through this process would see "location history" was turned off?

A Correct, if they opened the "more options" tab to see that.

So, moving on. I'm not going to set up a pin to the device. Then it's asking us to wait another second. It also then, on the next screen, says "review additional apps." It asks if you would like

to add these three other Google applications immediately to the device upon setup. Just due to them automatically downloading and updating, I selected that they not be downloaded. And we pressed "okay."

These final screens are referring to registering your device with the manufacturer, which is ASUS in this case. You can either create an account using an existing account or skip this function.

Moving to the next screen, still dealing with the ASUS account, whether or not you want to register, sign in, or register by Google ID, or you can skip.

On the next, it determines what data --

THE COURT: To be clear, you didn't undertake any of those options?

THE WITNESS: No, ma'am.

THE COURT: All right.

THE WITNESS: Those functions are not directly related to Google.

THE COURT: Okay.

A The next is accounts and sync for you to determine what accounts you would like to sync across your accounts.

THE COURT: Just so the record is clear, just say some of the stuff that's on the screen, please.

So back up, please.

THE WITNESS: Okay.

A So, on the screen you can add another account, you can sync data across your ASUS account, your exchange or email, as well as the application called Flickr, or your -- or the Gmail account that's selected here, and it is already preselected with the check to sync data for that account as you set it up.

Moving forward, it provides you with a prompt on the next screen for Google drive. It's a promotion to get storage from Google for your various information. We can skip this offer and move to the next screen.

We're finishing up the setup. This is where it tells you your device is now ready and you can make changes to your configurations in the settings area of the device. We'll click the check and move on to the next screen.

And the next screen is where it launches the device as you would normally see it as you were using it throughout the day.

Q So this is the normal setup process at this point. You've got a phone that you can use?

A Yes.

Q What happens when you click on Google Maps for the first time?

A So we've now made all of the selections to set up, and now we go to use the device. Here, once these initial pop-ups are done telling me kind of how to use my new phone, I'll go in and select Google Maps, which is an application already on the device.

Q Does it bring up a map immediately?

A It does not. So you will see the prompt here for "get the most out of Google Maps." It says that Google needs to periodically store your location to improve route recommendations, search suggestions, and more. You can opt in or skip.

Q What are the options? When it says opt in, it says what?

A "Yes, I'm in."

Q And the text, does any text on this screen mention location history?

A It does not.

Q So prior to this setting up the phone, we did see a screen with location history, and it was marked as --

A It was turned off.

Q It was off. And your understanding is that if you hit "yes, I'm in," what happens?

A Yes. If you select "yes, I'm in," it turns on Google location history.

Q And it doesn't mention location history in the text on this screen?
A It does not.
Q What happens when you click on "learn more"?
A It's a hyperlink to Google's website where all of the terms and conditions are located.
Q The entire privacy policy?
A All of the terms and conditions.
Q It doesn't direct you to anything specifically about location?
A No, but it is -- you can find it in there. It's there.
That's the end of the video.
Q So that is the end of the video?
A Yes.
Q Can you tell us, how long is that video? How long did it take you, the entire process, from start to finish here?
A Without stopping, 4 minutes and 45 seconds.
Q How many screens mention location history?
A I believe one.
Q And that was only if you clicked on "more options" and scrolled down; correct?
A Correct.
Q How many of them fully explained what location

history is?
A You would need to -- none. You would need to go look at the policies and terms.
Q Thank you.
So, the government says that we can function in modern society without enabling location services like this. Tell us, how did you get here today?
A I used my phone.
Q You were driving?
A Correct.
Q You used your phone to get directions?
A I did.
Q Did you look up where the courthouse was online?
A I did.
Q Did you plug it into Google Maps?
A Waze. Just about the same thing.
Q You didn't use a road map, did you?
A I did not.
Q Out of curiosity, when was the last time you used a road map?
A It's been quite some years.
Q You're a forensic examiner. You examine a lot of phones; correct?
A Correct.
Q How frequently do you encounter devices that are

also used for Google Search?
A Most.
Q What about Google Maps?
A Most.
Q What about Gmail?
A Very often.
Q And YouTube?
A Quite often.
Q How common is it for you to encounter phones with location services enabled?
A Pretty often.
Q What about location history, specifically?
A Typically, that's a hard function to see activated. It's not something you typically go seek out on the device to see if it's turned on. But based on the different returns that I see for Google account-specific requests, as well as these geofences, it's clear that a lot of people have this function activated on their devices because of how they show up in these returns.
Q Do you know what percentage of all devices use Google services?
A No, I don't.
Q Who would know that?
A I'm sure Google would.

Q Do you know --

THE COURT: I'm sorry. Say that again.

THE WITNESS: I said I would be sure that Google would know how many devices use their services.

BY MR. PRICE:

Q Do you know what percentage of devices have location history enabled?

A I don't.

Q What about web and app activity?

A I don't.

Q What about Google location services?

A I don't.

Q Who would know the answers to those questions?

A I would be certain that Google would have statistics on their services being used.

Q Thank you.

I want to turn now to the scope of the geofence warrant here.

THE COURT: Before you get there, if you enable YouTube or Google Search when the default has gone to location history off, do you get any kind of pop-up? Does it change the default?

THE WITNESS: So, across the platform for location history, it's my experience that that prompt comes from Google Maps, but there are certain, as far

as YouTube and things like that, other prompts for them to want to track the web and app activity and things like that that all fall into those categories that Google explained earlier or have explained in their brief.

THE COURT: But I'm asking specifically about location history.

THE WITNESS: So, no, they do not -- I have not seen them promote location history.

THE COURT: Do you know whether or not the default changes?

THE WITNESS: No, I do not.

THE COURT: You don't know?

THE WITNESS: I do not.

BY MR. PRICE:

Q When you were reviewing information about Android version 8 and you came across screenshots of the various prompts here, we saw one that looked just like this; right?

A It's the same screen, besides the sign-in information at the bottom with your account.

Q Were there other prompts that you discovered in your research that trigger location history enabling, such as when you go to photos, my places, for example?

A Nothing that directly activated location history.

Q In the sense that they didn't mention it specifically here?
A Correct, it's not mentioned as location history.
THE COURT: Is it activated?
THE WITNESS: It does activate the sharing of location data for that application but not directly linking the activation of Google location history to that selection.
BY MR. PRICE:
Q I want to turn to the scope of the geofence warrant and the question of whether it was really limited to 150 meters. How big was the geofence here, according to the warrant?
A I believe it was 150 meters.
Q I apologize for making you do math, but do you know what area that is in terms of square meters?
A I don't think I looked up square meters. I sometimes look it up on Google just to figure out how large of an area it is.
Q Would it surprise you if it was 70,686 square meters?
A No, that wouldn't surprise me.
Q Do you have an idea what that translates into in terms of acres?
A I did try to look it up in acres. It's about

17 acres.
Q Did the bank take up all 17 acres?
A No, it didn't.
Q What else was inside that radius?
A There was a parking lot -- well, a large parking lot, a church, and I believe the back of a hotel or very close to the parking lot and one side of the hotel was also encompassed in that circle.
Q I'd like you to return to Exhibit 3, that raw data on the spreadsheet there. Go to the same page you were on before, which is page 4 of the PDF itself.
A Okay.
Q Take a look at column F.
A Okay.
Q What's the label on column F?
A "Source."
Q What does that mean?
A It is telling you what type of calculation was made. So here it displays either Wi-Fi or GPS was used to provide a location.
Q So those are the two sources of location data at issue here?
A That is provided in the data, yes.
Q Do you know how many data points came from Wi-Fi here?

A There were quite a few. Probably out of the data, I believe over 600.
Q Would it surprise you if it was 605?
A No.
Q Okay. And that means how many came from GPS?
A There were quite a few. It was more than 60 or 70, I believe.
Q Would it surprise you if it was 75?
A That sounds about right.
Q So the percentage of the initial geofence warrant -- the percentage of the initial geofence returns that came from Wi-Fi, what would that be?
A Over 80 percent.
Q Would it surprise you if it was 88 percent --
A No.
Q -- coming from Wi-Fi?
Okay. Which is more accurate, Wi-Fi or GPS?
A GPS.
Q So based on your training and experience with Google location data in other cases, can you tell us, generally speaking, how Google uses Wi-Fi to locate somebody?
A Yes. So the phone is constantly scanning for Wi-Fi access points, so a router. It's constantly scanning and seeing the signal strength from those

access points. Based on the signal strength and Google doing a lot of work to understand where each of those access points is, they can generally understand where you are located based on several points, giving a specific distance to that point. So, several of those put together helps determine a location for the device.

Q Is it possible, because this data is coming from Wi-Fi with its own range, that the step 1 returns here included devices that were actually outside of the 150-meter radius?

A Yes.

Q Why? How does that work?

A So, of course, the signal coming from the Wi-Fi routers isn't bound by that arbitrary circle that's drawn. They can spill out farther. Google doesn't know the exact position of every Wi-Fi access point. So if it's off by where it thinks the access point is, that provides kind of an error in accuracy as far as where it thinks it is. So if the access point reaches out farther, it could think that the phone was in the circle if it saw that access point versus being outside.

Q What's the typical range of a Wi-Fi network?

A About 150 feet is kind of a general estimate.

Q So, how far outside the radius might the initial search have reached? Twenty-five meters?
A It possibly could have, yeah.
Q Fifty meters?
A Possibly.
Q So, step 1 can actually include devices that are up to 50 meters outside of that radius. Do you know what the effective reach, the effective area, of the geofence warrant was here?
A It makes it quite larger.
Q Surprise you if it's 125,000 square meters?
A No.
Q Which would be about 30 acres; is that correct?
A It's probably going to go up quite significantly by adding that extra area.
Q If you add that extra area, what else was inside the effective range of this geofence warrant besides the church and the bank?
A You would include the -- there's a mini store -- or a self storage north of the bank and church. Probably more of the hotel and hotel area. The road going past the church. There's a business across the street, the wooded area behind the church. There's quite a bit of stuff in that area. If you kept expanding, you would just keep --

Q What about residences or apartment buildings? Would it reach some of those, too?
A It possibly could have. There is a set of apartments that kind of backs up to kind of the back side of the bank, but there's a wooded area there.
Q Right now we're talking about theory, though. You don't actually know where any of those Wi-Fi access points are located; right?
A No.
Q Who would have that information?
A Google possibly.
Q Why do you think so?
A Well, they've got to have something to base the -- you know, they've got to know the general area of the access point to use it as a reference to derive location. With the GPS system, the reason we're able to determine location is because we know where the satellites are. So it's a point of reference to then find yourself.
Q And here we don't -- what's the equivalent to the satellites? We know where the satellites are, so we can figure out our GPS location?
A This would be knowing where the actual access point is.
Q And we don't know where those are?

A No, we don't know which points were used.
Q Have they been provided to you by Google?
A No.
Q What would having that information allow you to do?
A You could use their various functions to -- if you knew the access point that was used, its location, signal strength, you could, in essence, kind of recreate or at least see what the results are. Here we just see the results.
Q Would it allow you to figure out how many hits were likely outside the 150-meter radius to begin with?
A It could.
Q Do you know the range of the Wi-Fi access points in this case?
A No, not specifically.
Q Would Google have that information?
A I don't know that they would have the range.
Q Certainly it hasn't been provided to you, has it?
A No, it has not.
Q If you did have that range, what would it enable you to do?
A I don't know that we would ever get the range, and I don't know that range would exactly assist other

than knowing, you know, kind of how far some of the access points may reach. You would never end up with an actual range.

Q But it would allow you to try and figure out how far outside of the 150-meter radius some of those reach?

A It could. If you could determine just how far away you could actually see the church's Wi-Fi, it could be quite a bit of distance outside of the circle just based on how close they are to the outer edge of the circle.

MR. PRICE: Your Honor, do you have any follow-up questions?

THE COURT: Let me make sure I understand that.

Why don't you restate what you just said.

THE WITNESS: So if the -- again, the circle that has been drawn around this area for the search to be given to Google, that circle doesn't limit really anything other than Google in their search. Out in the actual -- in this area, if you went and looked, the church's Wi-Fi, which the church is located within the circle, their Wi-Fi could extend out past the circle. And due to that, those measurements could be taken and actually place you in the circle even if you

weren't in the circle.
BY MR. PRICE:
Q So, if I can clarify. Google doesn't know where the location -- doesn't know the location of the access point for the church's Wi-Fi; correct?
A They generally know where it is, but not down to the specific, exact -- you know, they couldn't walk into the building, I don't think, and point it out to you.
Q But they have a general idea where it is, and they know that it's in that circle; right?
MR. SIMON: Your Honor, I would ask that he stop leading the witness.
MR. PRICE: I'm just trying to clarify your point, Your Honor.
THE COURT: I think I understand.
MR. PRICE: Okay. I'd like to move on, if that's all right.
BY MR. PRICE:
Q I want to continue asking you about the scope of the warrant but shift slightly and talk about Google's process, Google's algorithm for determining device location. So, you just talked generally about how Google uses Wi-Fi to locate devices, but do you know mathematically how Google actually does that?

A Generally, I know the process, but know how they label a display radius or how well they determine the accuracy of their calculation, no.
Q What would you need to know to figure that out?
A I assume we would just need to know what Google knows as far as how they actually process this data to determine how accurate it is.
Q How would you describe that process? Is it an algorithm?
A I honestly don't know.
Q Why don't you know?
A It never -- I just don't know their inner workings. Again, I know generally how it operates, but we don't know the fine print here that they have labeled out as to how this works.
Q And if you did know the fine print, what would it enable you to determine in this case?
A It could possibly determine a little more information as to how accurate it is but, again, without knowing what they possibly have or could tell us, I don't know.
Q Would Google have documentation about how this process works?
A I assume they do.
Q Have you seen it?

A No, I have not.
Q What do you think those documents might tell you if you did see them?
A I honestly don't know. I guess it would outline their policies and procedures on how they're going to conduct a search, how they apply anonymity to these devices and, really, all of the background work that they do.
Q What would it tell you about how far the search may have reached beyond 150 meters?
A I don't exactly know, but, I mean, it could provide some insight into that.
Q To the Wi-Fi access points?
A If they can provide that, yes.
Q Was any of that information in the warrant or the application?
A No, I didn't see any type of request like that.
Q Has any of it been provided to you?
A I haven't seen anything.

THE COURT: So, by the application, you're talking about Defense Exhibit 1?

MR. PRICE: Yes, Your Honor.

THE COURT: Now, Mr. Price, we've been going for a little while here. Do you have a while more to go?

MR. PRICE: I'm afraid I have a little bit more, Your Honor.

THE COURT: Okay. That's fine. I think we should take a little break just to be sure that everybody is fresh. So we're going to take a 10-minute break.

I'm going to remind you, sir, that you will remain under oath. Don't speak to anybody about your testimony or listen to any commentary about it. And I'll ask anybody here to do the same.

We'll just start fresh as if we didn't take a break. All right? So let's take a 10-minute recess.

(Recess taken from 12:30 p.m. until 12:45 p.m.)

THE COURT: All right, sir. We'll resume your testimony.

MR. PRICE: Thank you, Your Honor.

BY MR. PRICE:

Q Mr. McInvaille, I'd like to turn to the question of whether the data provided by Google in steps 1 and 2 is truly anonymous?

A No, I don't believe it is.

Q We're going to talk about it, but thank you. So Google says that the data produced to law enforcement here is in anonymized form. You reviewed it. Can you take a look again at Exhibit 3 and tell us what you

see?
A Yes. So they provide device identifiers, date, times, locations, the source of that, and then a radius inside of that data.
Q So you said device identifiers. Can you tell me -- column A. Take a look at column A and the column numbers in the far left. What are those numbers?
A That is the anonymized device ID.
Q Do you know what Google does to anonymize this data?
A I don't know specifically.
Q Do you know their process?
A I do not.
Q Why don't you know?
A It's not -- I don't know that it's published.
Q Would Google have that information?
A I'm sure they do have it.
Q What about the latitude and longitude coordinates in columns D and E?
A That's the estimated location of the device.
Q Are those masked in any way?
A No.
Q So that's the actual location data here?
A Yep. To their knowledge and to ours, yes.

Q What were you able to do with this supposedly anonymous information?

A With the step 1, you can take the information and, by device ID, plot out each of the devices and their locations that were returned in that first step. And then in the second step, it is the same devices but with an expanded time frame and the absence of a restriction on location.

Q So you took these latitude and longitude coordinates from columns D and E, and you did what with them?

A You can plot them on the map. I organized them by the device IDs.

Q So did you do that here? Did you prepare a demonstration for us?

A I did. There's a subset of those in a demonstration.

Q Let's talk about what you did for that demonstration. You made a visual representation of some of this data provided by Google?

A Correct. So I took -- by device ID, I mapped out each of the locations provided. And we did that in two steps. So you have the first step that shows the location for a particular device during the first step or the first return from Google.

We then take that same device ID and now use the data that was returned based on the step 2, which removed the circle, the limitation as far as location, and the expanded time frame, and then you can see general movements for a portion of that data.

Q So this visual representation of some of the data, here you made a short video?

A Yes.

Q Two minutes and 46 seconds?

A Correct.

Q And you have that video on a DVD marked Exhibit 5?

A Yes.

Q Have you reviewed that DVD before coming into court today to verify that it is the same one as the video that you made?

A I did.

Q And you marked the DVD with your initials reflecting that?

A I did.

MR. PRICE: I would like to move to admit the video into evidence as Exhibit 5 and remind the Court that this is under seal because it is based off of the same raw data.

THE COURT: All right. No objection?

MR. SIMON: No objection, Judge.

THE COURT: All right. It's entered under seal.

MR. PRICE: Thank you, Your Honor.

(Defendant's Exhibit No. 5 is entered under seal.)

BY MR. PRICE:

Q Mr. McInvaille, can you please walk us through what we are looking at here?

A Okay. So this is device ID 965610516. This is the stage 1 request information that came back on that number.

THE COURT: Can you say the device number again?

THE WITNESS: Yes. It's 965610516.

THE COURT: Okay.

BY MR. PRICE:

Q And for our purposes today, how do you want to refer to this?

A This is the -- the color is the easiest. So this is green. What you'll see on the map is the locations that we've been discussing throughout. The circle, which is in red, represents the geofence that was laid on the map, as well as a green dot with a date and time, of which that was the estimated location for that device at that time.

Q Where's that dot located?
A For this particular map, it's there on top of the -- which is the church.
Q All right. Why don't you go ahead and play it and tell us what happens next.
A The video will sit here for just a moment so that you can see the beginning. So, I'll pause here. We're moving back in time now. So, in the stage 2 request, we kept the same device identifiers but now expanded the time frame to before and after the incident, as well as removed the location restriction.
THE COURT: So this is a stage 2?
THE WITNESS: Correct. So this would have been -- this would have been the data -- the data used to create this portion here was from the stage 2 production that Google made.
THE COURT: So it's the broader time frame before and after. And what's the other distinction?
THE WITNESS: No location restriction. So instead of just asking for inside of the circle, there was no restriction on this request.
THE COURT: How do we know that?
THE WITNESS: I believe it's indicated in the search warrant. That would be the next step, or -- it was either there or in the email request. I can't

recall right offhand.

THE COURT: All right.

A So the first point that shows up is at 3:50 p.m. that afternoon. And you see that the dot is located on top of the hospital. I believe it was Johnston-Willis, if I'm correct. There at the hospital. And what you'll see at the beginning is several points are located in a cluster at that location prior to leaving that location. And I'll start now.

You see several of those points appear. And then now we see them begin to move away from that location, and they will move in a southern direction.

BY MR. PRICE:

Q Tell us, what does the increased spacing indicate to you?

A Definitely there was some travel from the area of the hospital down south to now where you see the original circle where we saw in the very beginning.

So, in this portion here, you will notice the kind of general direction of travel as well as the timing of that travel.

And in the next portion, you will see where --

THE COURT: Why don't you put those numbers on the record.

THE WITNESS: Okay.

THE COURT: The timing. Down south is down a road, which I think is marked as Commerce Road?

THE WITNESS: I can give them, yes, ma'am.

THE COURT: And then it returns to the church. So what kind of time frame is that in?

THE WITNESS: So, this is 28 seconds in the video. And you will see the first dot in the northern portion of the frame is at 4:36:59. The next being just south of that. And I don't recall the name of that. It looks to be Courthouse Road, possibly. The next dot is at the intersection of Hull Street and Courthouse at 4:39 p.m.

THE COURT: I don't want to identify who the user is. I just want a sense of the timing. So, you say you see there's travel. Is it five minutes? Is it 30 seconds?

THE WITNESS: I understand.

From the intersection of Courthouse Road and Hull Street, there is -- to the next point is about -- just over four minutes. And then arrives at a residence.

THE COURT: Okay. Now, what I'm really trying to get a sense of is how far the distance is, without specifics, and how long it takes. So, for

instance, Johnston-Willis Hospital was not in the red circle; correct?

THE WITNESS: Correct.

THE COURT: Do you have an estimate of how far outside the red circle it was?

THE WITNESS: Bear with me one second. More than seven miles.

THE COURT: All right. That's the kind of general information I'm looking for. Okay?

THE WITNESS: Yep. Moving into the area, once it comes down south towards the circle, you have -- from the time it gets here to then in the circle and then past the circle is about three -- excuse me -- four minutes and some seconds, and then moves even farther down to a particular residence.

THE COURT: And the residence is also outside the circle?

THE WITNESS: Correct, it is.

THE COURT: All right.

THE WITNESS: So once it gets to the area of that residence, you will see again another cluster of points showing up indicative of that device stopping at that general location.

THE COURT: Okay.

BY MR. PRICE:

Q Can we just summarize what happened with Mr. Green here?
A Yes.
Q Where did Mr. Green start?
A The hospital up north.
Q And then he drove south?
A Correct.
Q And passed by the bank, the church, what?
A So it appears, based on the timing -- I'll scroll back here. It appears, based on the timing of those three points, that the device was passing by. So not that it necessarily had to stop inside of the circle when it shows up. That dot that you see inside the circle at 4:41:45 is the one that shows up in the stage 1 return.
Q And that's inside the church or the bank?
A It shows on top of the church.
Q So after passing by the church, after showing up on the church, you said it settles on top of a single-family residence?
A It does.
Q Were you able to determine whose house that was?
A I reviewed tax records for the county and determined some names for that location.
Q And were you able to include -- draw a conclusion

about the likely identity of Mr. Green?
A Not necessarily the exact identity, but generally a family, I assume, who lived there.
Q Would that information be identifiable to law enforcement as well?
A It could be, yes. They're resources to look at.
Q Let's go ahead and take a look at the next one.
A So, moving to the next example, this device ID is 907512662. And what you see on the map is the -- is a single dot on top of the church. And what this is is the return for that device ID during the stage 1 production by Google.
THE COURT: And it's blue?
THE WITNESS: Yes, it is.
BY MR. PRICE:
Q Why don't you go ahead and --
A So, in the beginning of now the data for that same device ID that begins prior to the incident, it shows up at the apartment complex just to the south of the circle, less than a thousand feet away. And during that time, you'll see -- as it begins, you'll see several points show up in that general area of the apartments. And then shortly after, you will start to see a trend in movement to the north, likely by the road there beside the church.

Based on the timing, you have about a minute and eight seconds, or so, until the -- from the time the device is last showing at the apartments to the south where it originates up until the point that it gets up to -- towards Hull Street.

When we continue, it begins to move down Hull Street before making another trend down to the south towards another residence. So once we get down to this other residence farther south of the circle, we see several dots appear on a single-family residence here. Remains there just a bit before leaving and heading back north.

THE COURT: Before doing what? I'm sorry?

THE WITNESS: Before heading back north. And in the video, you'll see it returns back to the beginning location at the apartments.

And just for reference, Judge, just about -- it appears to be over a mile away from -- the residence is -- from the circle down south.

BY MR. PRICE:

Q Can you walk us through the chronology here like you did with Mr. Green? Can you walk us through the chronology for Mr. Blue?

A So, blue begins at the apartments here shown on the map, leaves in a northern direction, very likely

up the road beside the church, heads up to Hull Street. Appears to head to the right on Hull Street before coming back and making a southern travel down to that house that's a little over a mile away from the circle. And then after making that visit, returns back to the apartment complex where it began.

Q So what were you able to determine about the likely identity of Mr. Blue from this data?

A So, blue is a little more difficult just due to it originating in an apartment complex. As we all know, many people live in an apartment complex, and this is not precise enough to show which apartment is being used.

But based on the other travel to that known location, the single-family residence down south, determining identity of those individuals based on tax records and other open-source information, that, in conjunction with other open-source means, could help you determine who could have left from the apartment complex.

Q Let's talk about those additional databases.

THE COURT: Before you get there, how long of a period of time did this cover in tracking the blue dots?

THE WITNESS: Both -- all of these, based on

the stage 2 request, are all an hour before the incident and an hour after. So that's how it's bracketed.

THE COURT: Well, this particular one.

THE WITNESS: It's very close to that. It appears the first point shows up at 3:55 p.m. The final showing up almost 5:50 time frame.

THE COURT: Okay. And is there any spot for the blue example that appears inside the circle other than the step 1 return information?

THE WITNESS: No, ma'am, it does not.

THE COURT: All right. I'm done.

BY MR. PRICE:

Q Based on your experience as a law enforcement official, are you aware of any additional tools that may be available to law enforcement to help identify somebody based off of this open information that you have?

A Yes. We had information like Sky X and Linx that we could use to search names, locations, things such as that, that would help during an investigation, trying to identify people based on places that they frequent.

THE COURT: You're going to have to describe what those are and maybe spell them.

THE WITNESS: Okay. Linx is L-i-n-x. It's essentially a database that we had access to. People's -- different agencies' reports and things would go in there so you would be able to search names and vehicles, things like that, so you could see past history on different people based on if they were involved in different things.

BY MR. PRICE:

Q And one of those different things, would that be a traffic ticket?

A Yeah, it would be as simple as a traffic ticket or just filing some type of report from something being stolen. It could be really anything, any interaction with local law enforcement or anybody who entered that data into a report.

Q And something like that would give you an address associated with a name?

A Yeah, you could have several identifiers. You could have varying things from addresses to vehicles.

Q Did that happen in this example?

A Was that requested?

Q When you were looking at the data for Mr. Blue, did you come cross any records of one of those incidents?

A So a name that was listed under tax records for

the residence that was visited down to the south, one of those individuals did have where they had paid a traffic ticket in the past just a few years back. Same address.

Q So, would law enforcement be able to figure out the identity of Mr. Blue using these tools?

A I think generally you could, based on the combination of information. Again, it would -- not so much down to maybe the specific person, but I think you could narrow it down to a very small group of people based on these locations.

Q Thank you.

Can we turn to the final example here?

A So, here in the third example, we're looking at device ID 1305167661. On the map you will see three yellow dots. They also have corresponding times.

These dots show up at the -- either both -- there are two on the bank and then one right beside the bank. And then, again, we're going to move into stage 2 of the request and see the data prior to this, earlier in the day, for this same user.

Q So we're going back one hour now?

A Yes. So this starts at 3:51 p.m. And what you'll see is a data point again on top of a single-family residence. And for a moment here, you will see

several locations show up there at that same residence prior to moving just a short distance north.

THE COURT: So is the single-family residence outside the circle?

THE WITNESS: It is. In just a moment when this zooms out, I can tell you the approximate distance.

Just after being at the single-family residence, it moves just a very short distance north to this location, which is the Manchester High School there on Bailey Bridge Road. It appears to show up there in front of the school for just a brief moment before continuing north.

I would say it's approximately three or four miles from the circle is that original location.

BY MR. PRICE:

Q So the single-family residence where this starts an hour before the incident is how many miles from the --

A A few. Three or four miles at least.

Q Okay.

A So, continuing, you'll see the trend north as it moves towards the red circle. So then you see that device move into the circle there at the original dots that we spoke of that show up at the bank, which would

have been returned in the stage 1 request.

As we continue, you will then see that device move out -- move away from the circle and then move over to another kind of business area there on the same -- on Hull Street for just a moment before heading back south to its original location down at the single-family residence. And, again, that happens in that same time period as we've been speaking about.

Q So, can you just summarize the chronology for Ms. Yellow as well?

A Yes. So, again, that device starts out south of the red circle at that single-family residence, moves up towards the area of the Manchester High School. Continuing north after that and going to the bank. Leaving the bank area, going to some other -- in the general vicinity of those other businesses on Hull Street before returning back to the original location of the home.

Q So based on that information, were you able to draw a conclusion about the likely identity of Ms. Yellow?

A So, again, I started with tax records for that residence, located a name for an individual there. Also looked at that individual's information on Facebook and was able to see a group, a family, a

husband and wife, who also have a high school-age son in some of their pictures, referenced some of his ROTC events. So, yeah, I would say that, generally speaking, we were able to determine a likely group of people that that device belongs to.

Q And would this information be as identifiable to law enforcement as it was to you?

A Sure.

Q Even in this anonymized form?

A Yes, it is.

Q Thank you.

THE COURT: Let me just make clear. Of the yellow points that you have just indicated, how many other than the three that showed up at step 1 or stage 1 are inside the circle?

THE WITNESS: Just those three.

THE COURT: All right. Thank you.

BY MR. PRICE:

Q So, do you agree with Google's characterization of the step 1 and step 2 returns as anonymous?

A I do not.

Q Why?

A Our location and our frequent locations or our trend of locations in a particular amount of time is indicative of our identity. Individuals, different

groups of families even, you know, go to different places. So, yeah, our location is part of our identity.

Q Why does Google describe it as anonymized, then?

A Because all they did was strip away the unanonymous ID that can later be revealed. That's all they stripped away.

Q Do you know how they came up with the anonymized figures here?

A I don't.

Q Do you know if they have any relation to the actual Google ID?

A I don't know that.

Q Why?

A I haven't seen it published.

Q Would Google have policies and procedures that are relevant to this question?

A I would assume they do.

Q Why do you think so?

A They receive many of these requests a day, a year. I would think that there's some process or, you know, policy that dictates how these will be responded to and searched.

Q What might those policies tell you?

A Kind of hard to say. I'm sure, again, it would

dictate how they do the request, what they deemed acceptable based on the request. It could be anything.

Q And has any of that information been provided to you?

A Not that I've seen.

Q All right. Thank you.

So, I want to turn briefly to the question of voluntariness here. I seem to have misplaced a page. Here we go. I'm sorry.

So, we talked a lot about step 1. I want to turn now to steps 2 and step 3 and the question of how law enforcement worked with Google to narrow the 19 initial hits down to 9 and then 3. Can you tell us what occurred at step 2 in this process?

A So step 2 ended up being 9 of the original 19 that showed up in the circle. And then for that nine, they expanded time frame again to an hour before and an hour after and removed the geographical limit.

Q Have you reviewed any of the correspondence between law enforcement and Google about this request?

A I have.

Q Can you turn to the document marked as Exhibit 6 in your packet?

A Yes.

Q Do you recognize the document?
A Yes, I do.
Q What is it?
A It's an email between -- I believe it's Detective Hylton and -- as well as the -- it just says the Google team. So I assume Google's legal response group.
Q And it's the correspondence that you've reviewed in this case?
A Yes.

MR. PRICE: I'd like to introduce that into evidence as Exhibit 6, please.

THE COURT: Any objection?

MR. SIMON: We won't object, Your Honor.

THE COURT: Okay. It will be entered.

Just for the record, Hylton is H-Y-L-T-O-N.

(Defendant's Exhibit No. 6 is admitted into evidence.)

BY MR. PRICE:
Q In this request for step 2 data, starting from 19, how many users does Google -- does law enforcement ask Google to provide additional information on in step 2?
A It appears all 19.
Q All 19. Okay. So, step 1 was 19, and step 2 they also requested all 19, expanded data on all 19?

A It is with, you know, another sentence that if they feel it's unreasonable, that they may use the numbers that are listed 1 through 9.

Q Who's "they" in that case?

A I'm sorry?

Q Who's "they" referring to?

A "They" being -- Hylton appears to be the author of this email. So he advised that they could, if they saw that this request was unreasonable, that they could use 1 through 9 if it fit more likely.

Q "They" being Google?

A Oh, Google, yes. I'm sorry.

Q So, Google is the person who's going to determine what's relevant. Okay. Can you turn to Exhibit 7, marked Exhibit 7?

A Okay.

Q Do you recognize the document?

A Yes, I do.

Q What is it?

A Another correspondence between Hylton and Google.

Q And that's the correspondence that you reviewed in this case?

A Yes.

MR. PRICE: I'd like to introduce that as Exhibit 7, Your Honor.

THE COURT: Any objection?

MR. SIMON: No objection, Your Honor.

(Defendant's Exhibit No. 7 is admitted into evidence.)

BY MR. PRICE:

Q Can you tell us what that document says?

A Again, it says it's writing to inquire about my correspondence on 7-1 and 7-2. It's, again, requesting the same -- it's the same exact request, just a follow-up on, I assume, a nonresponse from Google.

Q And how many users does that ask for additional data on?

A The request doesn't change. All they did was add the paragraph at the top. So, the 19, but still with the added piece that you could just do the 1 through 9.

THE COURT: Use the language correctly. It says "If this request seems unreasonable, please keep in mind that Google device numbers 1 through 9 may fit the more likely profile of the parties involved." You don't need to paraphrase it. You should say it. Thanks.

BY MR. PRICE:

Q I'd like you to turn to Exhibit 8 in your packet,

please. Do you recognize that document?
A I do.
Q What is it?
A Again, correspondence with Hylton and Google team.
Q And this is concerning which step of the process?
A Still appears to be the step 2, but it has now been just narrowed down to devices 1 through 9.
Q Do you have any idea how law enforcement --
THE COURT: Well, first of all, is Exhibit 8 being moved into evidence?
MR. PRICE: Oh, yes, Your Honor. I'm sorry.
THE COURT: Any objection?
MR. SIMON: No objection, Your Honor. I don't think it's on the screen.
THE COURT: It does need to get on the screen.
MR. PRICE: It is right now.
THE COURT: Pardon me? It's not on the big screen.
THE CLERK: It just takes a minute once it's admitted.
THE COURT: Got it. That's why it wasn't on, because it wasn't admitted. So that is also entered. Thank you for doing it correctly. All right.
(Defendant's Exhibit No. 8 is admitted into

evidence.)

MR. PRICE: Thank you.

BY MR. PRICE:

Q Mr. McInvaille, do you know how law enforcement finally narrowed their list down from 19 to 9?

A I don't know the specifics, no.

Q Why don't you know?

A It's not in the correspondence that I've seen.

Q Did any of those nine seem like odd choices to include to you?

A I'm trying to remember the color. The color was blue, I believe. That, if I had to say, blue is an odd entry into this group.

Q Were there any others?

A Really, the -- I mean, honestly, once you -- well, for the stage 2, both green and blue would have been odd for the moving to the stage 9 process.

Q Why did the inclusion of Mr. Green in the stage 2 process strike you as odd?

A There was just one single point at the church.

Q At the church, not the bank?

A Right.

Q And compared to other people?

A Some -- there were others that were -- that showed up at both the church and the bank. There were some

that just showed up at the bank, and then there were a few that only showed up at the church with just single points.

Q So who would know why law enforcement included Mr. Green in stage 2?

A I'm not sure.

Q Would law enforcement know?

A I assume they would.

Q Would Google know?

A They may if they had discussion with --

THE COURT: You said they would or would not?

THE WITNESS: I assume they would.

BY MR. PRICE:

Q Would the magistrate judge who issued this warrant know?

A Oh, I don't know.

THE COURT: I'm sorry. You're sort of looking down.

THE WITNESS: I'm sorry. I don't know.

THE COURT: You don't know?

THE WITNESS: No, ma'am.

THE COURT: Just to be clear, can you identify what numbers blue and green are on the list?

MR. PRICE: With the corresponding device ID?

THE COURT: Yes.

THE WITNESS: Yes. Green is 965610516. Blue is 907512662.

THE COURT: And can you look at the list and identify which ones those are in 1 through 9?

THE WITNESS: Yes. It is -- the green is number 5 on the list. Blue is number 8 on the list.

THE COURT: All right.

BY MR. PRICE:

Q Let's talk about step 3 here for a second. You reviewed the correspondence with Google about step 3?

A Yes, I believe so.

Q Can you turn to Exhibit 9, please, in your packet? Do you recognize the document?

A Yes.

Q What is it?

A Another email from Hylton to Google legal team.

Q And that's the correspondence you reviewed in this case?

A Yes.

MR. PRICE: I'd like to introduce that as Exhibit 9, please, Your Honor.

THE COURT: Any objection?

MR. SIMON: No objection, Judge.

THE COURT: All right. It will be entered.

(Defendant's Exhibit No. 9 is admitted into

evidence.)

BY MR. PRICE:

Q What additional data did the government receive from Google in step 3?

A I'm just going to read it. "Please send subscriber information for the above device IDs as soon as possible."

So they asked -- law enforcement asked for the subscriber information for all three devices, device IDs, listed in this request.

Q Can you turn back to the raw data in Exhibit 2, please? Oh, I'm sorry, Exhibit 3. And the first page of the last return, it is the fifth from the last page. It says "Stage 3 Return.CSV" at the top. Sorry. The fourth from the end.

A I have it.

Q Do we have it on the screen? Great. Can you tell us what is in column A?

A Column A is the Gaia ID.

THE COURT: To be clear, this is a two-column listing, which differs from the earlier listings that had several, A through F or E. This just has A and B, and it has four rows under it.

Sorry to interrupt.

BY MR. PRICE:

Q Do you know what a Gaia ID is?
A It's what they call the Google accounts ID, administration ID.
Q So, what's the significance of providing the Gaia ID in this case?
A So, this is the unanonymized number now. In this column here, it's displayed as a formal just because of how the table was printed. So that's not the full number.
THE COURT: I'm sorry. Google accounts what?
THE WITNESS: Google accounts ID administration.
THE COURT: Okay. Pardon me.
BY MR. PRICE:
Q And you're saying that the plus 11 in all of those numbers indicates that the number is actually much longer?
A Yes, it is.
Q And that gives a -- corresponds to the pseudonymous device IDs?
A Correct. So, you have the Gaia ID, which is the actual ID for the user. In a corresponding column to the right of that marked device ID, which is what we've been seeing in the stage 1/stage 2 requests, and that is the anonymous number. So now what it's

giving you is it's labeling the anonymous number with its real number now so that it can be identified.

Q Do you know how law enforcement narrowed the list of nine down to these three?

A No, I don't.

THE COURT: Do you know who narrowed it down to three?

THE WITNESS: I believe Hylton was the requester for that.

THE COURT: Okay.

BY MR. PRICE:

Q Did any of these three seem like odd choices to include to you? We just talked about --

A Yep. So, the device ID ending 2662, which was the blue example that we reviewed, that is the ID that you see earlier in the day at the apartments passing by the -- on the road there past the church and then returning back to the apartments. That ID made it to the final three.

Q Why did it strike you as odd that that ID would make it to the final three?

A From looking at the data, it appears that the device only passed by the location, not having time to stop. It just doesn't appear that there was time in there to even stop through the geofence based on the

data that was given in stage 2.
Q Do you recall what time of day Mr. Blue hit inside that geofence?
A It was 4:35:45.
Q How many minutes was that before the incident?
A I believe about 20 minutes. I don't know the exact time. I think it was just before 5:00.
Q So he only hit once in the church 20 minutes before the robbery?
A Correct.
Q But he was included in the final three here?
A Correct.
Q Do you know why law enforcement might include someone who wasn't at the bank or in the parking lot?
A I'm not sure.
Q Do you know who might know?
A I assume Hylton, since he made the request.
Q What about the magistrate judge who issued this warrant?
A Oh, I have no idea.
Q So, you can't tell, based on the information you have, how the government went from 19 down to 9 down to 3?
A No.
Q What would you need to know?

A I assume their thought process as to what constitutes needing to know more about each dot that shows up.

Q So you'd want to know how the law enforcement officers made their determinations here?

A Yes. I would assume that there's a reason behind choosing certain IDs over another.

Q Anything else you would want to know?

A I'm sure that would be helpful, just the reasoning behind it, and just the application how it was -- how the data was applied to the map to get an understanding of what it was telling you.

Q All right. Thank you very much.

THE COURT: I want to ask one question about these exhibits. These communications, Exhibits 6, 7, 8, and 9, is there anything on the exhibits themselves to identify the date and time they were transmitted?

THE WITNESS: No, I do not think there are. The only one that has any reference of date and time was one of the follow-up emails that references a prior request on 7-1 and 7-2, but that's all.

THE COURT: All right. Thank you.

MR. PRICE: No further questions at this point. Thank you, Your Honor.

THE COURT: All right.

Mr. Simon, do you anticipate a long cross?

MR. SIMON: Judge, I think probably between 30 and 45 minutes.

THE COURT: Why don't we, then, just take, again, a 10-minute recess just so that we can all catch our breath. I do appreciate that you all showed up timely. I want to be sure that we keep things moving, and so it will just be ten minutes. I have 2:26. And I'll ask you all to be back again. Sir, you will remain -- I'm sorry. 1:26. Daylight Saving Time happened.

Sir, you will remain under oath, and I'll advise you again, don't speak to anybody about your testimony, and I'll ask everybody here not to speak to him. All right? Ten-minute recess.

(Recess taken.)

THE COURT: All right. Mr. Simon, are you prepared for cross?

MR. SIMON: Yes, Judge.

THE COURT: I remind you that you are under oath, sir.

THE WITNESS: Yes, ma'am.

CROSS-EXAMINATION

BY MR. SIMON:

Q Mr. McInvaille; is that right?

A Yes, sir.

Q Good afternoon.

A Good afternoon.

Q Mr. McInvaille, you've been called to testify in this hearing. And your testimony, if I understand it correct, is that you have -- you have to opt in in one form or another into Google to collect your location history; is that correct?

THE COURT: Now, Mr. Simon, you're definitely going to have to be closer to the microphone. It's natural to look at the witness, but when you do that, your face is away from the microphone.

MR. SIMON: Understood, Judge. And my apologies.

BY MR. SIMON:

Q Mr. McInvaille, you've been called to testify in this hearing today. And, as I understand, your testimony on direct examination was on a few fronts. First, you say on location history the user has to opt in for the collection of that location history; correct?

A That's correct.

Q And your testimony with respect to the clarity about that location information -- if we could pull back up exhibit -- Defense Exhibit 4 and just go to the end of that video and pause it.

A The very end?

Q Yes, the very end of Defense Exhibit 4.

A Okay.

Q Okay. And so once that clears off the screen, can you read what -- this is the 4-minute-45-second mark of Defense Exhibit 4. Can you read for the Court what's there on the screen there?

A Yes, sir. It says "Get the most from Google Maps." Then "Google needs to periodically store your location to improve route recommendations, search suggestions, and more. Learn more." And then the indicator is "yes, I'm in" or "skip."

Q And you didn't click the "learn more" box in this simulation; is that right?

A Not in the video, no, sir.

Q Okay. But if you did click that "learn more" box, you'd be told about what type of information they're storing, how long they're storing it; right?

A It takes you to the Google terms and privacy agreements. It takes you to their website where all of that is located.

Q So if you wanted to know, you could know; right?
A Correct.
Q It's clearly on that screen; right?
A That's where you would navigate to it, yes.
Q And with respect to your work with geofence warrants -- you testified that you generally work with geofence warrants. Can you say that with more clarity? How many times have you examined a geofence warrant?
A I don't know about how many times. I've looked at several throughout several states. I see them quite often in North Carolina where I do a lot of work. A dozen.
Q Okay. A dozen. And so your understanding -- right? -- is that there are three steps; correct?
A Well, that's what they outlined in the brief, yes.
Q Okay. And you've looked at the search warrant in this case in Defense Exhibit 2; right?
A Correct.
Q Okay. And in that process, there's a multistep process. Step 1 is going to be from 4:20 to 5:20; is that right?
A I believe so, yes.
Q Okay. And that's going to be what we've been talking about as inside the box; right?

A Correct.

THE COURT: Wait a minute. What are you referring to?

MR. SIMON: We're referring to Defense Exhibit 2, Your Honor. This is the search warrant in the case he was testifying to earlier about the difference steps --

THE COURT: The search warrant is Exhibit 1. The Google amicus brief is Exhibit 2.

MR. SIMON: My apologies, Your Honor. I've been asking the witness about Defense Exhibit 1. My apologies.

THE COURT: That's all right.

BY MR. SIMON:

Q And I'm referring to what would be, essentially, the fourth listed page of Defense Exhibit 1. That'll be attachment 2. It starts as attachment 2 and basically outlines this process, this three-step process. First step is going to be inside that 150-meter radius; correct?

A You're on page 3?

Q I'm just asking you about the search warrant.

A Yes, it is.

Q Okay.

THE COURT: Well, he's allowed to look at the

documents.

MR. SIMON: Understood, Judge.

THE COURT: So, you should give your answer based on the documents.

A I just thought you referred me to a page. That's just what I was clarifying.

BY MR. SIMON:

Q Okay. And so stage 1 gives you points that are inside of that 150 meter radius; correct?

A Correct.

Q And then law enforcement can get additional location information for 30 minutes before; correct?

A Yes.

Q And then 30 minutes after; correct?

A Correct.

Q And that's stage 2; right?

A Correct.

Q But in stage 1, you only get points that are inside that radius; correct?

A That's correct.

Q All right. Now, you've been testifying a little bit about the anonymous nature of the returns in this case. And the raw data is Exhibit 3, but I won't necessarily walk you page by page through that. But you've testified about a Mr. Green, a Mr. Blue, a

Mr. Yellow; right?
A Correct.
Q And Mr. Green, in your three-pass video, Defense Exhibit 5, that starts at about the 28-second mark and it ends 1516, the identifier. You don't know who Mr. Green is; correct?
A No, sir.
Q And Mr. Blue, that starts at about, I think, the 1 minute and 50 second mark of Defense Exhibit 5. You don't know who Mr. Blue is; correct?
A No, sir.
Q And with respect to Mr. Yellow, that starts about the 2 minute 27 second mark of Defense Exhibit 5. You don't know who Mr. Yellow is; correct?
A No, sir, I don't.
Q And that means they're anonymous; right?
A No, not that they're anonymous. Just that I can't positively identify the person.
Q But your testimony to this Court today under oath is that you don't know who Mr. Green is; correct?
A I do not know.
Q And Mr. Blue, you don't know him; right?
A No.
Q Mr. Yellow, don't know him; right?
A No.

Q Okay. Now, you've been in law enforcement before you joined Envista. You're with Envista now; right?
A Correct.
Q Okay. And when you were with law enforcement, you wouldn't go to a judge or place in an affidavit that you can get a search warrant on a home based on the data you reviewed in stage 3 at stage 1; correct?
A From which stage?
Q Let's say stage 2. Stage 2. You wouldn't go get a search warrant based on this information that you plotted in Defense Exhibit 5; correct?
A Not from stage 2, no.
Q Okay.
THE COURT: A search of what? Of which data point?
MR. SIMON: Well, we're talking about -- we can go one by one, Judge.
BY MR. SIMON:
Q Mr. Green -- this is at the 28-second mark that began. The testimony on direct examination was that this was a single-family residence that you went back to; correct?
A Correct.
Q And based on what you reviewed at stage 1 and stage 2 about Mr. Green -- this is the identifier, the

anonymous identifier that ends 1516 -- you wouldn't go and get a search warrant based on that information; correct?

A No, I would not.

Q You would need to know more; right?

A Yes.

Q And the same with respect to Mr. Blue. You said Mr. Blue went back to an apartment; correct?

A Correct.

Q And then he went to another residence; correct?

A Correct.

Q And you wouldn't get a search warrant for either that apartment complex or that home based on those returns; correct?

A No, I wouldn't.

Q Okay. And that's because you don't know who they are; right?

A Correct, or what you would be searching for.

Q Now, with respect to Mr. Yellow, again, with the single-family residence, you wouldn't try to get a search warrant based on that information; right?

A No.

Q You would want to know more?

A Yes.

Q Okay. And speaking to wanting to know more, you

were talking about being a bit befuddled as to why they might be looking at all these other people -- right? -- at stage 2 and stage 3; correct?

A Correct.

Q All right.

MR. SIMON: Can we pull up Defense Exhibit 6?

BY MR. SIMON:

Q Defense Exhibit 6, do you see that first listed number there that ends with 5659?

A Bear with me.

Q I'll give you a minute.

A Yes, I do.

Q Okay. Let's look at Defense Exhibit 7. Do you see that first listed number in Defense Exhibit 7, do you see that?

A Correct.

Q That's the same as that first listed number in Defense Exhibit 6?

A It is.

Q And then Exhibit 8, Defense Exhibit 8, this is when it's narrowed down to nine; correct?

A Correct.

Q And what's the first listed number there? It's the same one as the first listed in Defense Exhibits 6 and 7; correct?

A Correct.
Q And now let's look, finally, at Defense Exhibit 9. The first listed number is the same as the first listed number in 6, 7, and 8; correct?
A Correct.
Q Did you plot that number?
A I did.
Q Okay. And what did you come to find out about that number based on your expert opinion?
A There were points within the area, of course inside the circle, in the initial request. Those were both at the church and the bank. And the stage 2 portion of that same person's data, it shows travel from that area south, away from that area. I don't exactly recall the exact area to describe it, but south, away from the circle.
Q So based on your expert opinion, looking at this case, in your expert opinion, is that the device that likely was involved in the crime here?
A Yes, it could have been.
Q Okay. Now, with respect to your understanding of Google, you're here to testify about materials that Google might turn over; correct?
A Correct.
Q That the defendant wants Google to turn over;

correct?
A Yes.
Q You never worked for Google?
A No.
Q Okay. To the extent that you've worked with Google, have you seen them provide, in a geofence warrant, any additional information than what's been provided to the United States here?
A I've never seen it requested.
Q You've not -- well, let me rephrase. Have you seen -- the stage 3 returns you've seen in this case; correct? The stage 3 returns you've seen?
A I have seen them, yes.
Q You've seen the longitude and the latitude in this case?
A Correct.
Q Okay. And you know it's a geofence warrant; right?
A Correct.
Q You've worked with some other geofence warrants; correct?
A Correct.
Q Are all of those from Google, all those geofence warrants?
A Yes.

Q And Google has provided the same information; correct?
A Yes.
Q Okay. Nothing different; right?
A I mean, besides the particulars of the case, no.
Q Besides the fact that it's a different crime committed elsewhere; right?
A Yes.
Q And different devices then available. In those cases, not all of them, but let's say the vast majority of them, they were prosecuted; correct?
A I mean, either they are or are currently being, yes.
Q Okay. Now, with respect to the specific request made in this ECF No. 28, you've reviewed the motion for discovery that the defendants filed; is that right?
A I don't know about the motion.
Q But you have been made aware of the different requests that the defendant is making in this case; right?
A Correct.
Q Okay. And your testimony earlier was that some of this could be helpful; right?
A Yes.

Q Might be helpful; correct?
A Yes.
Q Are you familiar with the facts of this particular case?
A Not the entire case, no.
Q Are you familiar with the fact that a search warrant was executed in this case on three residences?
A No, sir.
Q Are you familiar with the fact that there's eyewitness testimony placing a blue Buick behind the bank?
A No, sir.
Q Okay. So, you're not familiar with the facts of this particular case; correct?
A No. I've been -- this is what I've looked at.
Q So, when you say it could be helpful, you say that on a blank slate; right?
A Yes, just in terms of the request itself, yes.
Q Okay. Now, let's talk about one of the holy grail requests, it seems. You were talking about an algorithm; correct?
A Correct.
Q And that algorithm, to your mind, you would be able to crack Google's case, know exactly what they're doing and how they're doing it; right?

A Sure.
Q Okay. Would you know how to do that?
A Probably not.
Q Okay. So, your testimony in this case under oath to this Court is that this information should be provided by Google, but you personally could not do anything with it; correct?
A I don't know that I can, but I would assume it's quite complex.
Q Okay. Too complex for you to get?
A Could be.
Q Okay. Are you prepared to -- it seems that in talking about Google, your testimony is at no point going to be that you know anything for a fact; correct? With respect to Google?
A From like -- from --
Q In terms of the requests that the defendant has apprised you of, that they've made you aware of that they want from Google, your testimony has consistently been could be, may be, but you don't know; correct?
A Correct. We don't know what we can get from Google because we don't know what process, policies, documentation they have on the process.
Q And because of that, you can't actually sit here and tell us what would be helpful; right?

A Correct.
Q Okay. Now, I'm going to jump back a little bit here. You've been qualified as an expert here, but I want to talk to you a little bit about your training and expertise. We received your C.V. in this case. I'm sure you're aware of that; right?
A Yes, sir.
Q Okay. And you've received approximately 100 hours in location training; correct?
A Somewhere in that area. I don't know the exact number.
Q Okay. But would it sound correct to you if I told you that approximately half of your training came from Envista Forensics, your employer? Correct?
A Correct.
Q All right. And Envista is a company -- as far as you're concerned -- right? -- you're going out and you're just testifying primarily for defendants across the country; right?
A We do plaintiff work. We work both sides in civil cases as well as criminal cases.
Q Okay. How many cases have you testified in for a prosecution of a defendant?
A None as an expert in Envista.
Q But when you were in law enforcement, you did?

A Correct.
Q Okay. Now, the stage 3 returns in this case, that's going to be the returns that come -- that's going to be the raw data we get. I'm sorry. That's not the stage 3. The raw data that we get in this case that has the latitude and longitude; right?
THE COURT: Which one are you asking about? Are you asking about Exhibit 3 or stage 3 returns?
MR. SIMON: I'm -- Judge, it's actually -- the stage 3 return is also the Defense Exhibit 3. So, that's just the three levels of that return that's under seal.
BY MR. SIMON:
Q And I'm asking, just generally, about the latitude and longitude coordinates in this case. You could plot those; correct?
A Correct.
Q And you were testifying on direct examination, essentially, that the Google information in this case is 100 percent accurate; right?
THE COURT: Wait. Wait. Wait. I want to be sure I understand what you're doing.
MR. SIMON: Sure.
THE COURT: The stage 3 return has two columns, A and B, the G-A-I-A ID the device ID. It

doesn't have latitude and longitude that I can see. So if you're offering that presumption, you need to tell me the basis of it.

MR. SIMON: Your Honor, you've corrected me. I'm talking about the stage 1 and 2 returns as a part of the geofence. I'm saying stage 3 because in my mind, I'm just thinking about the latitude and longitude, but that's incorrect.

THE COURT: Which is not in stage 3 at all.

MR. SIMON: Correct.

THE COURT: So we've got to make the record clear.

MR. SIMON: Correct. And I will correct myself.

BY MR. SIMON:

Q The stage 1 and 2 returns, they are Defense Exhibit 3, that's going to be the latitude and longitude coordinates for a certain number of devices; correct?

A Correct.

Q The stage 1 was for 19; right?

A Correct.

Q And stage 2 was for 9; right?

A Correct.

Q And with respect to your testimony on direct

examination in Defense Exhibit 5 -- and I'm not asking for it to be pulled up, but in Defense Exhibit 5, you put particular points at particular places; right?

A Correct.

Q Now, if you'll look with me at column G there, the map display radius, it's your understanding -- right? -- that Google is approximating this information; correct?

A Correct.

Q So, when you testify on direct examination to this Court and you say this is where the person was at this time and I know it for 100 percent certainty, that's not correct; right?

A It's an estimated location of the device.

Q But your Defense Exhibit 5 doesn't show that it's estimated; correct?

A That's what I testified to.

Q Defense Exhibit 5 shows a particular point at a particular place; is that correct?

A That's the latitude and longitude provided.

Q Okay. But the display radius here, it's your understanding that Google tells you that a certain point could be within a certain display radius; right?

A Correct.

Q Okay. And so Defense Exhibit 5, if it were to

impress upon this Court that it is a point at a particular place at a particular time, you wouldn't actually say that; right?

A No. It's an estimation of the device's location.

Q Okay. So, Defense Exhibit 5 isn't accurate; right?

A It's accurately plotted based on the latitude and longitude, yes. That dot does not mean that the device is exactly on top of that dot.

Q But if I look at Defense Exhibit 5 -- and we can pull it up if you'd like -- Defense Exhibit 5 indicates that it is a particular dot at a particular point in time; isn't that right?

A Again, from the latitude and longitude.

Q Okay. But that's how it is plotted in --

THE COURT: That's asked and answered. You've made your point.

MR. SIMON: Okay. Understood, Judge.

BY MR. SIMON:

Q With respect to those points and the accuracy thereof, wouldn't that inform your discussion of the anonymous nature of the returns in this case?

A As far as how big the radius is?

Q Correct.

A Yes, it could.

Q So, if you see a radius is a certain circle, you wouldn't be able to say that because it's here, I know for certain that that's where I should be checking; right?
A That's correct.
Q You'd check the next place; right?
A You could have to check multiple, yes.
Q Check maybe the block; right?
A I don't know about the block, but, yeah, it could be more than one place.
Q But you'd give consideration to column G? You'd say let me look at what that display radius is; right?
A Sure.
Q Just to be clear, your understanding of the display radius is that it's giving you the sort of plus and minus on accuracy; right?
A That's their approximation of within this area.
Q Okay. Now, you were in law enforcement for a period of time. How long were you in law enforcement?
A Eight and a half years, I believe.
Q Okay. Eight and a half years. And in your time in being in law enforcement, if you were to get sort of the stage 1 and stage 2 returns that law enforcement received in this case, you would assess multiple points over a period of time; correct?

A Correct.
Q And you would assess those points for a number of reasons; right?
A Sure.
Q You would assess maybe whether you could look into some further connection with the potential perpetrator of the crime; right?
A Correct.
Q You'd maybe check if they -- you'd look at it to see if maybe they could be a witness to a prosecution; right?
A That's possible, yes.
Q And if you knew that there was evidence in a case that showed the potential -- or the perpetrator of the crime, they had a phone to their ear, you might say let's see who else is there, see if they have a connection to that robber; right?
A Correct.
Q So when you are befuddled at stage 3 and stage 2 when there are multiple devices requested, that befuddlement comes because you don't really know all the facts of this case; right?
A Correct. I'm looking at the data and how it comes out.
Q Okay. Now, just to be clear, the data in this

case, its accuracy can be assessed at this point in time; right?

A Based on what they have provided, you can see -- I mean, they're giving you their determination of how accurate they think it is.

Q Okay. But if you had the algorithm, you wouldn't be able to do anything with that; right? We've established that.

A It's possible. We don't know.

Q Okay. With respect to the anonymous identifier from Mr. Chatrie in this case, the anonymous identifier, as you understand it, is going to be the column that's in the far left corner of Defense Exhibit 3; correct? That's going to be column A at the stage 1 and stage 2 returns?

A Yes, it can be located in there.

Q And that's the anonymous identifier for these folks?

A Correct.

Q All right. And so presumably, if there's evidence in this -- or if there's argument in this case made by the United States that a particular account was at a particular place in time, you could plot the coordinates for the anonymous identifier related to all these accounts; right?

A Correct.
Q And you could see which account would match up to the allegations by the United States; right?
A Yes. And if you're talking about from stage 1 to the final stage, you can compare those three, yes.
Q And you could find out who that account belongs to, by your testimony, if you were to get at least the -- well, let's just talk about stage 3. If you get the subscriber info, you know who it is; right?
A Right, it provides subscriber information.
Q But until stage 3, you don't actually know who has what account; right?
A No, sir.
Q And that's the stage where the United States only got three subscribers; right?
A It's stage 3, correct, yes.
Q And, again, about that stage 3 piece, you testified on direct that you were again -- I'm using the word "befuddled" -- but you were a little surprised that Mr. Blue ended up in stage 3; right?
A Correct.
Q And -- but, as we've talked about, there might be multiple reasons to look at an account; right?
A There could be, yeah.
Q So it's not just that the United States or

Mr. Hylton here would be looking at who committed the crime; right?
A It's possible.
Q You'd be looking at maybe who also had some other involvement; right?
A Correct.
Q And that's what you would do when you were in law enforcement; right?
A Correct.
Q Okay. You'd run to ground everything you could?
A Sure.
Q Okay.

MR. SIMON: Nothing further, Your Honor.

THE COURT: Redirect?

REDIRECT EXAMINATION

BY MS. KOENIG:

Q A few questions, Mr. McInvaille. Thank you for your testimony today.

I wanted to make sure that I understood what you were saying in response to Mr. Simon's questions. You've worked on several geofence warrants; is that right?
A Correct.
Q Or cases involving geofence data.

A Correct.
Q And did you say that just the teams that you've worked with have never sought this extended discovery that we have sought here?
A Correct. I've never seen it requested.
Q And when did you first start seeing, in your practice, these geofence warrants come about?
A I believe I have one from a 2017 case.
Q Would it be logical, then, to see more litigation as a new technique comes out?
A Absolutely.
Q And if we were able to go -- let's go through -- so, in going through -- you testified on cross-examination that we don't know exactly what we would be able to get from Google until we ask for it; right?
A Correct.
Q And if we were able to get information from Google that indicated how they came up with this process, how would that inform our ability to look at the legality of this warrant that they sought?
MR. SIMON: Objection, Your Honor. I don't know what his basis would be to know the legality of it.
THE COURT: I actually think that calls for a

legal conclusion, and he's not a lawyer.
BY MS. KOENIG:
Q How would that inform our understanding of the data?
A It could help you understand, of course, these display radiuses, how they determine that that's what they approximate. It could tell us more about the -- for instance, in the Wi-Fi, if they record what Wi-Fi was used to generate those points. Several of those items could help you better understand how they came up with the data that they provided.
Q Let's break it down a little bit. So, you've talked about how Google provided an estimate of the display radius; right? Do we have any way of checking that with any degree of certainty?
A No.
Q And the only way we can get that is if we get the method that Google used to create that radius; right?
A Correct.
Q And is that what we generally think would be encompassed in the algorithm?
A I would assume so, or at least their processes of generating this evidence.
Q When we say "algorithm," what do we kind of mean?
A I think more than, you know, than we're looking at

some elaborate mathematics here, that it's more of just maybe what you guys are referring to and that we've been talking about. It's more of their underlying process of taking unknown data or their location history data and turning it into what we see here.

Q And then going -- you know, you were able to talk with us about a couple of examples of Mr. Blue, Mr. Green, Ms. Yellow as to what we think a path of travel may indicate; right?

A Yes.

Q And if we were able to have the access point, if we knew that you had an access point, what would you then be able to do to help us assess the accuracy of the data that's indicated to come from a Wi-Fi source?

A That would just give you the known location that Google used to approximate this location. Then you can -- if you wanted to, you could go try to determine those locations, try your best to determine if it was -- if it seems like an appropriate estimate of the location or not.

Q And if you have the Wi-Fi access point, would you be able to take some kind of a device and go out and map the range of a Wi-Fi source?

A To an extent, yes, you could go find out where the

access point is and where you might be able to access it from.

Q And so, for instance, if we were able to get data from Google that indicated that a device ID had connected with the hotel Wi-Fi access point, could you roughly map out the range of the hotel Wi-Fi access point?

A Again, knowing the location of whatever access point was used, if it still exists and is there and has not been changed, you could generally determine maybe how far away from that location you could be and still connect to it.

Q Would that enable us to better understand how some individuals who appear to be passing by this area of the red circle, how they possibly got captured into the circle even though the data indicates that they may not have actually stayed at that location?

A It could help, yes.

Q In terms of -- and I want to go back to Defense Exhibit 1, which is the warrant --

THE COURT: Before you go there, I just want to be clear. As to Defense Exhibit 3, column G says "Maps Display Radius (m)." Can we confirm that it's meters?

Q Do you understand that to mean "meters"?

A Yes, it's meters.

MS. KOENIG: Thank you, Your Honor.

MR. SIMON: That's my understanding, Judge.

THE COURT: Okay. I just want to be clear.

MS. KOENIG: Sure.

BY MS. KOENIG:

Q When we are talking about the warrant itself, is the warrant indicating to the judge that they obtained this warrant from, is the application for the warrant indicating that they are looking for suspects?

A Yes, I do believe it is.

Q You don't recall any mention to the judge, "Well, maybe we're going to look for witnesses to the event" -- right? -- by trying to get this geofence data?

A Bear with me just a second. I know it asked for unknown subject. I don't recall about others. Bear with me. The quotation there references other people, but that was a quotation, I believe, that they alleged by the suspect, but -- I don't know that -- bear with me. I may not see it, but -- I don't see anything that refers to, based on what the law enforcement wrote, that there is any mention of witnesses, but again --

Q Thank you, Mr. McInvaille.

Does it -- going back again to -- so, have you

actually plotted out all 19 people?
A Yes.
Q And have you plotted out the extensive data for all nine individuals?
A Yes.
Q Were you able to determine that the examples that we provided are not just isolated in the sense that it's not just these three individuals whose data appeared odd to you?
A When we say "odd," I think that's referring to just some of those that have single points within the circle and no other data to really go off of. And then based on once you see the larger set of data, you see a trend as though they're passing by. So that is what makes it appear that the point that references them into the documentation actually reveals their anonymous ID number in there.
Q When we're trying to get information from the law enforcement agents or the government about why they chose to narrow the 19 down to the 9, why is that? Why do we need that information? What does that mean to you?
A For me, it would help understand just the -- the reasoning behind certain people making it to certain points. For the case, that would help me understand

the -- you know, how things are playing out as far as this data goes.

Q And if you were better able to understand why the government did what they did, would you be better able to assist Mr. Price, and myself, and Mr. Chatrie, eventually, as to what this selection process meant?

A Sure.

Q And if we were to get -- so, you mentioned -- far earlier in your testimony today, Mr. Price had asked you, are you aware that Google does provide trainings on this geofence data?

A I don't know that it comes directly from Google, but there are places to get training that I've seen for Google location history services, that mix of data.

Q Was there at least one time where you tried to sign up for such a training?

A Yeah. I believe there was a webinar that detailed information about these types of requests and how to frame them and use them.

Q Were you able to successfully sign up for that?

A No.

Q Why was that?

A It was restricted to law enforcement only.

Q Did you then do some further checking and find

that Google -- that whoever is providing this information about the geofence warrants, that information seems to be restricted to law enforcement?

A From what I've seen, yes, it is.

Q Okay. And if you were able to access those training materials, would you anticipate that you would then be better able to understand how Google used this process and provided the information?

A I can only assume so, but I would assume a training on that particular subject could help in the understanding of different factors involved with these.

Q Likewise, that same thing with Google's policies and procedures about how they search the data and how they create this location data, would that also assist us in understanding if it existed, and it was provided, how this information applies in our case?

A Yes, because, I mean, you see the difference in what the government has asked but in comparison to what Google said in their brief as to what they provided. So there's something in place that kept them from fully responding. I don't know if that's the proper way to put it, but providing exactly what the government asked for.

Q Is it fair to basically sum it up to say that

there's a lot of questions that we have that you've done your best to answer, but you just can't because you don't have this data from Google?

A Yes.

MS. KOENIG: No further questions, Your Honor.

THE COURT: All right. Can this witness be excused?

MS. KOENIG: Yes, Your Honor.

MR. SIMON: Judge, could I just ask a few more questions on recross?

THE COURT: That's not our norm. Is there an objection from the defense?

MS. KOENIG: No, Your Honor, unless it elicits something else, if I could have the last word.

THE COURT: We're definitely not going down that rabbit hole.

MR. SIMON: That's fine. It's not a huge deal.

THE COURT: All right.

So, sir, thank you for your testimony. You're excused from testifying.

THE WITNESS: Thank you.

(The witness was excused from the witness stand.)

MS. KOENIG: Your Honor, the defense has no further witnesses at this time.

THE COURT: All right. Is there any evidence from the government?

MR. SIMON: Your Honor, no, we won't elicit any testimony.

THE COURT: All right. Well, I'll hear argument.

MS. KOENIG: Your Honor, could we take just a few minutes of a break? Mr. Price, he would love to eat a little bit of a sandwich first.

THE COURT: All right. We do not want anyone passing out in the courtroom.

MS. KOENIG: Thank you, Your Honor.

THE COURT: Again, I'm keeping it to ten minutes just to keep us on schedule.

MS. KOENIG: We can make that happen.

THE COURT: We'll take a ten-minute recess.

(Recess taken from 2:25 p.m. until 2:35 p.m.)

THE COURT: All right. I'm prepared to hear argument. I want to make one thing clear because both parties here were asking our witness, our expert, about what the judge decided. And I want to be clear, in Chesterfield County, magistrates are not judges. So this person who signed it appears to be David

Bishop. And as far as I recall, to be a magistrate in a county, all you need is a college degree. You don't even need a master's, and you definitely don't need a J.D. And because you all have been using the nomenclature "judge," I want to have you all respond to that, if you could.

MS. KOENIG: I think that the Court's recollection is accurate, Your Honor. I think we just get so used to seeing magistrate judges in this building sign off on warrants. It's a colloquial term, and it is does not indicate the person has a J.D. necessarily or significant legal training of any sort.

THE COURT: Well, I need something on the record about that. I think you have to have some kind of college degree. I think we don't know if this person has anything other than a college degree because the record is blank as to that.

MS. KOENIG: That's right.

THE COURT: All right. Mr. Simon.

MR. SIMON: Judge, I can't speak with 100 percent certainty as to rules in Chesterfield, but it is my understanding, as a general matter, that the Court is correct, that you don't have to be a lawyer with a J.D. or --

MR. DUFFEY: Judge, I'm sorry to interrupt. We would ask for time to check that because I know that used to be the rule, but something tells me they changed that, that there is a requirement. Could we file something?

THE COURT: Yes, I would want you to file it. Everybody referred to it the same way. So I'd prefer that you all, if you can agree to what the requirement is, file it jointly on the record.

MR. SIMON: Will do, Judge.

MR. DUFFEY: Let's do that.

THE COURT: I don't claim to know whether or not that's changed.

MR. PRICE: Your Honor, it is apparent that we are not dealing with an ordinary search warrant here. It's not an ordinary search. It's not an ordinary warrant. And it's also apparent that we are not dealing with an ordinary amicus. Nothing about this case is ordinary. And that is the point.

That is why the defense is requesting the discovery that we are requesting here. And it's also why we believe that the search in this case involves an unconstitutional general warrant that is infinitely overbroad and profoundly lacking in particularity.

Think about the extraordinary breadth here.

Google initially is searching all of its users in order to identify who might be in that circle. More than 1.2 billion of them. It is hard to imagine how you end up with a broader search than that regardless of who ends up in the circle.

But even that circle is not what it seems. And that's what we learned here today. Google says its data points are not facts but estimates. And if these are estimates, then we need to know how Google is making those calculations. We need to know what goes into it in terms of the inputs. That would be the Wi-Fi location points. As well as what Google does with that information. That would be the algorithm.

It's also why defense is asking for Google's policies and procedures in terms of responding to this. It is absolutely unclear to us why Google may have -- and we're not even certain they did -- why Google may have included only location history in this warrant return.

They have other types of location data. The government requested those in the warrant. The warrant does not specify location history versus some other type of location data. So there's a factual question lingering here about whether the data was

limited to that one category or not, and if so, why.

If it wasn't limited to location history, then we have a whole set of other questions about how voluntary that location data transmission was.

Location history, Your Honor, is arguably the most voluntary of the three. That's not to say it is voluntary in the Fourth Amendment sense, but as you can tell from the setup process, the first two types of location data, web and app activity and Google location services, are enabled by default and really require no affirmative action on the part of the user other that signing in with your Google account when you start up the phone.

So if those two types of data aren't at issue, then the argument about lack of voluntariness, for example, gets even stronger than it is here.

That also speaks to the lack of particularity in this warrant. Again, it is as unclear to us as it perhaps was to the issuing magistrate that this data would be searching everybody, that it would potentially expand beyond the scope of that radius. And, frankly, that it may not be as anonymous as the government and Google insinuate that it is.

The lack of particularity in this case cuts from beginning to end, from the information presented

to the magistrate about the scope of the warrant, about how anonymous that data really is.

In the middle, the government goes back to Google in step 2 and asks for additional information on all 19 users that were identified in step 1. It's not clear why they did that, but that certainly doesn't seem to be the thrust of the warrant and application that were presented. In fact, the warrant only says that the government will attempt to narrow it down. It is unclear whether they attempted here or what that attempt looked like. But in two instances, they went back to Google and asked for information about all 19 again. It doesn't appear that the government narrowed its request until the third time.

THE COURT: Well, to be fair, they said if you think the 19 is unreasonable, take the top 9; right?

MR. PRICE: And that is absolutely the language that we're focusing on here, Your Honor. It does appear that the reasonableness determination was left up to Google and not a judicial officer.

THE COURT: What's the upshot of that?

MR. PRICE: Well, the Fourth Amendment requires particularity in the search, that the government present all the information that it has

that's relevant to the judge. And the process of narrowing here is one of those limiting factors that a judge would presumably consider when deciding whether to issue a warrant like this.

So if there is a representation that the government is going to narrow down its list or that it's going to, in some way, limit the scope of what it asks for, that's information that needs to be presented to the Court, not to Google. And it's great that Google decided to, on its own, limit the scope of the step 2 returns, but that, unfortunately, does not absolve the government when it comes to particularity. The *Groves v. Ramirez* case decided by the Supreme Court just a few years ago made that point clear.

Even if the limitation, as a practical matter, comes from law enforcement or the responding party, that is not the same thing as a judge making that determination.

And the fact that it may cut one way in one case doesn't mean that it's not going to cut the other way in a different case, and that is why the determination is left up to the courts and not to Google.

THE COURT: Are you arguing at all about whether or not the fact that it was limited in some

respect -- you seem to argue it was limited by Google and not the government. Are you arguing either under Rule 16 that that suggests any kind of joint investigation or that under *Brady* it makes Google a member of the prosecution team?

MR. PRICE: So, our position here, Your Honor, is that Google did function as a member of the investigative team. And I think it is important to look at that in the broad sense. These policies and procedures do not appear to have been created in a vacuum. And the process of requesting data in steps and pseudo anonymizing it appears to be something that a lot of thought was given to. Our question is whether that thought and that process involved the government as well.

And it is unclear, for example, why Google may have chosen location history to provide as opposed to web and app activity or Google location services. Why?

I do believe that if we were to receive discovery from Google or the government about this process, this would likely not be the first time that Google and the government have talked about how the process should go.

So to the extent that Google is creating this

process, is responding to the government without any judicial intervention in between them, at least for step 2 and step 3, would seem to indicate that Google and the government -- at least for those steps, if not for the process more broadly -- were, in fact, working together.

And for Rule 16 purposes, that would subject Google to discovery in the same way that the government would be required to process discovery.

THE COURT: Well, let me ask you this: I told you at the beginning of this hearing that you were going to have to address the government's argument about 17(c). And so why aren't you just issuing a subpoena to Google?

MR. PRICE: Honestly, Your Honor, we considered it. And then Google interjected and decided to file an amicus brief in this case.

Our understanding of the way that Google has responded to subpoenas in the past has been to oppose them fiercely and to move to quash any sort of subpoena like this.

So we were, frankly, a little surprised but also happy that Google, on its own, decided to submit what we would consider to be an initial round of discovery, an affidavit, in the form of an amicus

brief.

And so at this point we would like the opportunity to follow up on that with them.

THE COURT: So why follow up now through justice argument rather than by issuing a subpoena?

MR. PRICE: If Your Honor feels it would be helpful, we would be more than happy to issue a subpoena to Google.

THE COURT: I don't give legal advice to either side, but I'm asking why you don't do it.

MR. PRICE: The reason that we didn't do it was because Google, in a somewhat extraordinary move, decided to come into this case on its own and provide an amicus brief with information relevant to some of the questions that we had in discovery. In fact, their brief does answer some of those questions. The problem is that it doesn't answer others, and it raises even more.

THE COURT: All right. Go ahead. Keep arguing.

MR. PRICE: I was going to say, even at the end of this process it is unclear how we get from point A to point B. It is not clear how the government went from 19 down to 9 to 3 requesting additional information about users who were, as we

learned today, pretty clearly unconnected to the crime.

If you have somebody who only hits once in the church, not the bank, and all of the other stage 2 data shows that that person was likely to be just driving next to the road -- on the road next to the bank, it does raise a question about why that person then advanced to stage 3.

Was the government just curious? It's unclear to us. And the fact that there is no judicial process after the warrant is signed initially I think raises serious questions about the propriety of the government or Google getting to decide which users get de-anonymized at the end. And especially given some of the candidates that made it to step 3, it doesn't appear that there is an obvious explanation. So we would like to know more information about how that process worked.

With respect to voluntariness, this is an issue because the government is arguing that there was no search here at all because this information was shared voluntarily with a third party, Google. In fact, what we learned is that that can be accomplished in a matter of minutes, in under five minutes, simply by clicking on "yes, I'm in" without any reference to

location history whatsoever.

So there is this factual question lingering here about how voluntary this is. How many people actually click "yes, I'm in"? That, to us, seems to be a pretty important fact to have here. And it doesn't seem likely that people are going into the depths of their settings on their telephones to enable location history specifically. So it raises the question: How is this happening? How is it happening if it's not really that intentional? And it does seem to be occurring through these pop-up screens. And so we want to know how common this is. Does this happen with most people or is it rare?

THE COURT: But what does that go to as far as what I have to decide? So, if you learn the percentages -- I'm looking at a motion for discovery under *Brady* and Rule 16. So, if you find out the percentages, what does that go to?

MR. PRICE: It ultimately goes to the merits of our suppression argument. The Supreme Court in *Carpenter*, for example, talked about the ubiquity of cell phones and the way that they are used today, the way that most people have them, they may as well be appendages. And if that is similar with respect to location history, in other words, if we were to learn

that 95 percent of users have location history enabled, it brings us much more in line with the reasoning in *Carpenter* about voluntariness. So that would be the relevance here.

The same goes for information about the inclusion of web and app activity and Google location services. So those are those other two types of data that Google supposedly didn't turn over. But if those were involved in this process, if they fed into location history, for example, then I do think we would be having an entirely different conversation about voluntariness.

THE COURT: So, one of the things I'm struggling with in this case is I'm going back to materiality, and I need you all to educate me about this a little bit. But materiality talks about, for instance, under Rule 16, whether or not it significantly alters the quantum of proof in the defendant's favor if the evidence is suppressed. Right?

And so is there a different kind of standard for materiality under evidence that would support a motion to suppress rather than evidence that supports information at trial, a defense at trial?

A lot of these cases are post trial, right?

And so we're dealing with something that might be a unicorn. I don't know if I've seen anything like it. I think if you had something dead-on, both of you would have given it to me, but I'm not sure that I see that.

So, is there a difference if you're trying to get information for a motion to suppress versus information for your actual defense?

MR. PRICE: So, we haven't, obviously, gotten into the trial phase of this case. In fact, Your Honor, we hope not to get to that phase and believe that this motion is, in fact, dispositive. And I believe the government actually agrees with us on that point.

If the defense succeeds on its motion to suppress, that will be the deciding point, I believe, in this case. And if the Court were to suppress the results of the geofence warrant, presumably that would entail the suppression of all the fruits thereof, and there would be no more case. So --

THE COURT: Well, that actually goes to another question that I have. I don't think that your brief included anything about fruit of the poisonous tree, but the United States made clear that there's this plethora of information other than what was found

through the geofence and the Sensorvault information that makes it -- I can't remember, actually, what they argued. I don't know if it's harmless error or -- it doesn't matter because there's just tons of information that otherwise shows guilt by a great degree.

MR. PRICE: I'm sorry. I don't have my suppression motion in front of me, but I am certain, Your Honor, that we asked to suppress both the results of the geofence warrant and their fruits.

And it is my understanding that the only way that the government came to have any physical evidence in this case was as a result of learning my client's identity from that geofence warrant, and that absent the geofence warrant, there would be no physical evidence.

If the government is planning to make an independent source argument, we haven't seen it.

THE COURT: All right.

MR. PRICE: I would add that it appears the government has the same question as the defense when it comes to the inclusion of only location history. It is certainly not what the government asked for in its warrant. And it appears that this is a policy that Google has internally. It is unclear to what

extent the government was aware of it, but it seems as if they were not here. And we are both wondering why Google responded the way that it did.

In short, Your Honor, I think we're -- what we're asking for, if I can sum it up, is fairly straightforward. It's the Google policies and procedures relating to geofence warrants. We want to know about location history versus web and app activity and Google location services. We want to know the percentage of devices that have these features enabled. We would like to know about the Wi-Fi access points and the algorithm used to determine an estimate of location based on that. And we would like information about the narrowing process.

Every one of those pieces of discovery goes to either breadth, particularity, or voluntariness. They are material, central to each one of those arguments. And to round out the point here, Your Honor, we believe the information about those is, well, required under both Rule 16 and *Brady*.

I understand your point about not having an ultimate outcome in this case, but if we tweak Rule 16 or interpret Rule 16 and *Brady* to mean the outcome of the suppression hearing and thus the outcome of the case, then we think under either standard we would be

entitled to the discovery we are seeking today.

THE COURT: So, the United States is basically saying there's nothing written -- I think their briefing says there's nothing written about what they do to narrow down the process. And so you just need to wait until the detective -- I think it was Hylton -- testifies. Why is that not correct?

MR. PRICE: So, we have asked the government for information about the analyst who did the work here. It's not clear that that was Detective Hylton. It's not clear what his process was. We would love the opportunity to discuss it with him and to discuss it with Google.

THE COURT: The analyst where?

MR. PRICE: Whoever for law enforcement was responsible for the narrowing process, what information they used to make that determination, presumably, in addition to what they received from Google.

THE COURT: All right. Okay.

MR. PRICE: All right. Thank you very much, Your Honor.

THE COURT: Thank you.

MR. SIMON: Judge, just to start where they ended, with respect to the culling down of the

anonymous identifiers, the folks we went from 19 to 9 on, Detective Hylton made that decision. And the Court was correct on our representation about that. That testimony will be provided, but there's no current documentation that would sort of fall within the ambit of discovery rules. And I think what we are doing in this case is commensurate with what is done in all cases. And rightfully so. There's no requirement to create a document like that. The testimony will be presented, and he will be cross-examined, I'm sure forcefully.

And with respect to any other analyst involved here, Special Agent D'Errico, who we were considering calling, certainly they will be provided expert notice as to his testimony. And the Court has already ordered that to be produced on February 3. So we will fall in line with the requirements there.

With respect to Detective Hylton, who did make the determination on culling them down, we will elicit testimony from him on that point, but there's nothing currently in hand.

With respect to Google, there is some discussion -- I think the Court hit the point straight on. Rule 17 provides a process by which you get documents from a third party if you want more than

what, in this case, magistrate order process, legal process provided. That is the standard.

It sounds like the defense counsel acknowledges that, is willing to undertake that process. And to the extent that it's difficult, I think that's neither here nor there for the Court. It's just a process that has to be undertaken and is considered in the Federal Rules of Criminal Procedure.

With respect to the point about Google sort of working hand-in-hand with the United States, that point's been briefed in this case. There's no -- there's really no -- how do I say it? -- sort of substance to that claim.

Google did what was required of it in relation to court-ordered magistrate order process. And the negotiation piece there, there were several emails brought to the Court's attention today. All of those indicate -- right? -- that there is some pushback potentially from Google. And certainly to the extent that we want something from them, we can't compel that from them personally. It all goes back to that search warrant.

But more importantly, the cases cited by the defendant sort of noting when a company like Google -- when a third party might be -- not a company like

Google, but a third party might be brought into the -- being a part of the investigative team for purposes of *Brady*, which is really the only point there, because we don't believe there's a constructive possession or a due diligence requirement under Rule 16. The most recent Fourth Circuit precedent is somewhat old, but it's very clear that there is no constructive possession. It's got to have been actual control.

And so we're clear there that --

THE COURT: The issue there wouldn't be constructive possession. It would be joint investigation under Rule 16.

MR. SIMON: Under Rule 16. But, Your Honor, my point is is that there is no joint investigative team precedent in this circuit under Rule 16 in terms of producing something under Rule 16. But we would concede that to the extent they were to be seen as an agent in this case for the government, much like, I guess, a special agent, we'd have to certainly produce documents created in that course. So I guess as a practical matter, it ultimately does extend to that *Brady* sort of joint prosecution consideration. But under Rule 16, the *Pinto* decision is clear. There's no -- when the bail bondsman right there has the document, says you don't have to get that, there's no

construction possession. They're not a part of your prosecution team or they're not a part of the prosecution.

And so I guess there is sort of --

THE COURT: Well, what the defense is saying is that it's a little bit fact bound, right? I mean, the cases that have dealt with this do suggest that, in the Fourth Circuit or not, do suggest that if the more sort of independence and collaboration that goes on between a third party and the government, the more likely it is considered under Rule 16 or under *Brady* to either be a joint investigation or the entity to be a member of the prosecution team. It's not quite as black and white as you say, I don't think.

MR. SIMON: Sure. And, Judge, just to -- and I understand the Court's point. Even considering that, even acknowledging the point about the fact-bound nature of the inquiry as to whether we turn over stuff in the possession of Google that we don't have, the cases cited by the defendant don't support their viewpoint. And we've briefed that point, but every one of those cases, one, there's no process mandated from a magistrate saying you have to turn this over pursuant to the Fourth Amendment probable cause being found under Rule 41 for this evidence, the

search warrant.

And certainly, unlike those cases, Google is not brought into this case to prepare documents for purposes of this investigation.

So, *McCormick*, I guess, is the case out of the Tenth Circuit, and all the other cases are state court decisions from California, but they all focus on folks who are literally brought into the prosecution for purposes of the prosecution, and the documents and anything they can provide is for purposes of the prosecution.

Just from a factual standpoint, Google is providing to us business records that they created in the course of their business that they provided and didn't create because the United States started investigating the defendant in this case. These are just documents that they had in their possession. So, that's a meaningful difference in terms of sort of how they come into this process.

And it would also go to the broader Sixth Amendment piece, which is kind of an argument made in the reply brief that these business records are not testimony for purposes of the Sixth Amendment. I think there's clear case law on that point.

Google is not involved in this investigation

because we went to Google and said, We need you to create some documents or do something for purposes of this investigation. What they had were business records that they turned over.

But even considering cases where there might be more of a sort of private hybrid, the cases cited by the United States, the decision in the Seventh Circuit, which I think is the *Gray* decision, which talked about sort of Indiana hiring a private entity to do some work on behalf of Medicare. And they had documents created in the course of their business that were relevant to the prosecution. They turned those over, but that didn't turn that private company into an arm of the prosecution and as part of the investigation.

There's also the more -- sort of the legal point here, which is the *Collins* decision in the Southern District of New York, which says you have to consider the fact that even if the United States wanted to go back and tell Google to turn this over, it's necessarily circumscribed by the basis upon which they got the information in the first place. Right?

So, in *Collins*, they wanted to go back and search -- they wanted -- the defendant wanted the United States to go back and search the computer of

somebody who had provided previous consent. And the District Court there said they can't do that. They have to -- they can't just tell the individual to turn over their computer. That would be much the same way.

I think Google has made it clear in this case that they respond to legal process. They don't respond to the United States saying, "Give us documents or else." They don't respond to the United States saying, "We're investigating something and thus you need to participate and help us out." And that's just the reality of the situation.

We had to -- we were required to get process, and that's what happened here. And that's why Google is engaged with this investigation at all.

And even with respect to the stage 2 -- right? -- so stage 1 you just turn over the coordinates inside the radius, and in stage 2 there's an attempt to narrow down to get additional location information. So, basically, a total of two hours of location information was gathered for only nine devices. But that second stage gives you 30 minutes before and 30 minutes after. So that's what defense counsel has referred to as that culling down process.

That process is set forth in the search warrant. And there's some discussion of what Google

turned over and why they sought to turn over certain documents. The numbered page 2 of Defense Exhibit 1, which is the search warrant in this case, particularly attachment 2, says Google will provide anonymized information regarding the accounts that are associated with the device that was inside the described geographical area during the time frame described above. This anonymized information will include a numerical identifier for the account, the type of account, the time stamp, location coordinates, and the data source that this information came from, if available. That's what was provided in this case.

We received latitude-longitude coordinates. We received a time stamp on them. We received the source; Wi-Fi, GPS, and otherwise. I think it's Wi-Fi and GPS. And so the search warrant's pretty clear about what's being requested.

And the bottom line as it relates to the possession, custody, and control argument, whether it be under Rule 16, which plainly lays that out, is that there's no case law supporting the premise. And the underlying premise is very simple. Once you get a search warrant, and once you serve it on a Yahoo!, a Google, an Apple, an AT&T, if they respond in accordance with that search warrant, they are part of

your investigation team.

And to the extent that there's a broad search here, there's a broad search also in those cases as well. I think to the extent that there's a second stage here, that would be the only argument that would really be any -- would provide any meaningful difference or any difference in this case. I don't believe it -- meaningful because, again, it's provided for in the warrant. There's no -- there's no Google correspondence with the United States with no regard for that warrant. So everything is circumscribed by that. And I believe the reasoning out of the Southern District of New York in the *Collins* decision is to that point, that the defendant has to acknowledge, even based on their own argument, that we can't just go to Google and tell Google to turn over an account without some legal process.

In this case, if you argue there's a reasonable expectation of privacy, that's a search warrant. And so we think it's clear that Rule 17, Federal Rule of Criminal Procedure 17, provides the basis upon which the defendant would get these materials from Google.

And both parties over the course of -- now I guess it's been a few months -- received an email from

Google's outside counsel, reaching out to both sides talking about the amicus brief. So we certainly have known who the sort of lead lawyer for Google has been for some time. And even before that the defendant knew who we had corresponded with, who the United States had corresponded with in terms of executing this warrant. And so that goes back to the *Cameron* decision from the District Court in Maine, which, again, I think, is insightful. They know who to serve the subpoena on. They've got it. And they can go about that process. Again, it seems that they've acknowledged that that is the path to take for a third party and to receive these documents. And should Google seek to quash that subpoena, that would be analyzed under Rule 17, and appropriately so.

THE COURT: If it is the case that they decide to issue a subpoena to Google, what happens next?

MR. SIMON: Judge, I think that's where this is, as the Court noted, a more difficult situation. It is a hybrid, right? So, the defendant has noted -- has argued that Rule 16 should apply in reference to a suppression hearing in terms of sort of this third-party request for materials.

The only decision cited for that is a

District Court decision that applied a 1970's Fourth Circuit decision that had nothing to do with Rule 16. I think that was cited in the *Cranson* decision out of the Fourth Circuit. It has nothing to do with Rule 16.

And what we know from the Supreme Court is that when we talk about materiality, we're talking about in preparation for the defendant's defense, the Supreme Court says that goes to rebutting the government's case-in-chief, and arguably you could say we certainly can see that the geofence warrant is how we know this defendant was the target of the investigation.

So, there could be an argument that that's enough to be a part of the government's case-in-chief as opposed to a constitutional claim, which we believe this is, that doesn't really go to the merits of the evidence against the defendant.

And so in *Armstrong*, that was a selective prosecution claim, said the prosecution shouldn't have been brought. It's unconstitutionally -- they proceeded on an unconstitutional basis or there shouldn't be a prosecution. And the Supreme Court made clear that there should be a different standard there when it comes to a claim like that. That does

not go to the defendant's defense. The defendant's defense is actually rebutting against the government's case-in-chief.

This is a little different because there's evidence -- there's evidence gathered from the search warrant in this case. So I'd acknowledge that.

But ultimately, this case can proceed, I believe, to a suppression hearing without ordering Google to turn these documents over. I say that for a few reasons, because there are undisputed facts. There are undisputed facts as to there being other Google users whose information was collected as a part of this warrant. Undisputed 19. It's undisputed that Google has many, many, many users. Probably can be part of the public record how many users Google has or how many people are sort of a part of Google's customer base.

Irrespective of how many, the Court's going to have to acknowledge that there are over certainly a million, and if we go to a billion -- I don't know the number, but it's out there how many people Google does business with.

It's also undisputed that we've got location information for these people that expands outside of the box for stage 2. All right. So we know that

there are nine people's information we received that was outside the box for stage 2.

There's been no evidence elicited in this case that any information received in step 1 was necessarily from somebody who was outside of the box of that stage 1 search warrant at stage 1.

And so I think the real facts that are at issue are really undisputed. We say there are a lot of Google users, that it's voluntary. Even their witness said yes, it's voluntary. And the question, the voluntariness question, to the extent it's informed by *Carpenter*, the *Carpenter* decision -- and, again, this isn't the suppression hearing, and we're going to argue that issue when it comes up, but the *Carpenter* decision talked about the ubiquity of using cellular telephones by powering them on and maybe them hitting off of a cell tower, and that this information occurs over, I think, a seven-day -- basically, the cell towers collect this information once you power the phone on. Everybody has to use it.

I don't think there's any argument in this case that you necessarily have to use Google to have a cell phone, certainly not to talk on it, certainly not to text on it, certainly not to travel. There are other applications to use to travel.

And so to the extent that the litigation needs to be prolonged for purposes of this information, I don't necessarily see it, but that ultimately would be an issue that Google addresses in response to a Rule 17 subpoena responding to whether this information is relevant, whether it's oppressive, and the other considerations that go with Rule 17. But it's my position that the Court can proceed to address the constitutionality of this warrant on the basis of certain undisputed facts as set forth.

I don't think this information from Google is going to give the Court any more understanding than what has been provided, that there are lots of users.

THE COURT: Let me ask you this: The defense said that there's an issue about it only being location history and not the other information. So, respond to that.

MR. SIMON: Again, the search warrant request for time stamp location coordinates and the data source for those coordinates, that's what this search warrant provided. It's not clear to me at all that that is somehow a material issue in this case. I mean, how would that be material to -- and the Court was asking about sort of how you apply that standard, but how would that be material to the accuracy of this

information? Because, ultimately, that's one of the pieces that goes to sort of the merits of the claim. What value would more points give us --

THE COURT: The expert testified that it doesn't normally just say location history. And I don't have anything to the contrary, right?

MR. SIMON: Judge, no, that -- I mean, what I can tell you is that what we -- certainly what he responded to in terms of this geofence warrant to get that, this is what Google provides, and there was some, I think, lack of clarity about what this search warrant asks for. But this search warrant says to provide the time stamp location coordinates and data source for each type of Google account.

There is another search warrant in this case that is for historical Google information. That's been made part of this record in this case, and there is -- there is some sort of web activity and sources like that, but that is sort of about the broader count. It's not clear to me that geofence warrants, at any point, provide more than what we've been provided here.

THE COURT: But he testified they do. It may not be clear to you, but you can't testify to this.

MR. SIMON: Well, Your Honor, I believe the

record will show that the witness, when asked whether the information provided in response to a geofence warrant has been in addition to what we have here, he said no. I think he did state that with respect to warrants that go to other types, when it's a user-specific search warrant, you know which account you're going after, then you get that additional information, but not with respect to the geofence search warrant.

THE COURT: Okay.

MR. SIMON: And, Judge, I do think that it is -- with respect to significantly altering the quantum of proof, I think the Court has that correct, that that has to be the standard. And with respect to how you apply that standard, it is backward-looking in a case where we haven't gone to trial yet, but I think it's undisputed that evidence was found at these three different locations, that there was a statement of probable cause, that there was certainly an admission post-Miranda in this case to the crime. And so materially altering the quantum of evidence from a Rule 16 standpoint --

THE COURT: You have to agree that the way you got there is through the geofence information.

MR. SIMON: That's right, Judge.

THE COURT: So it's a little bit problematic to say, Listen, once we identified the guy, then we knew which house to search, and then we got everything. Then the way we identified him was through the geofence warrant, but we're not going to say the geofence warrant is material because once we used it to go to his house, there was all this other proof. That strikes me as too much tautology for the government in this case.

MR. SIMON: And I understand that point, Judge, and I think that's correct, that the first -- we can't deny that everything else flowed from the geofence warrant.

Materiality goes to, I think, something more than just saying sort of what happens, like how material was the geofence warrant to the case. Materiality goes to whether we're going to be led, based on articulable facts, to something that is going to significantly alter the quantum of proof for this Court.

There is not a single request made by the defendant in this case that is going to significantly alter the quantum of proof because, again, we've agreed on certain basic points. Google --

THE COURT: Okay. I think I've got that

argument.

MR. SIMON: Okay.

THE COURT: All right. Is there any response?

MS. KOENIG: Very briefly, Judge. As it relates to -- because I think we've got two separate pieces. We have -- one is the information we're requesting from the government about how they made the process themselves to go down from 19 to 9 to 3. And that doesn't involve the question of getting Google involved.

THE COURT: So, you're away from the microphone.

MS. KOENIG: I'm sorry.

THE COURT: I heard about every fourth word.

MS. KOENIG: Sorry. I want to start with the first question, which is the information that we have sought from the government about how their actual investigators, Detective Hylton and anybody else that was involved in that process, narrowed down the scope of the data sought from the 19, to the 9, to the 3. That doesn't involve this issue about whether Google was on the investigative team. I think it's very clear that Detective Hylton would be a part of the investigative team.

THE COURT: Why isn't it enough that they say they don't have to create information for you, just wait until he testifies?

MS. KOENIG: So, we could do it that way. But the reason we cited the case that we cited, which is *Wilford* from the District of Maryland -- and this is at least the quickest place I can put my hands on it is in our reply brief, on page 9 of the reply brief related to the discovery motion.

And I think the mechanics of how this would work is we could do discovery finding on the stand, but what Detective Hylton would essentially be testifying to is I plotted all these points, and I had the 19, down to the 9, down to the 3, and here's the reasons why. We're then going to have to be able to very quickly -- and I don't know physically how we would do this because we would have to essentially have access to Mr. McInvaille's entire mapping process, which, you know, we showed you 3 pathways today, but there would be 19 pathways. And the reason I think that the *Wilford* court required the material information related to pretrial motions must be produced before the motions hearing is to ensure its effective use.

I think we would be wasting a lot of the

Court's time in some senses because we would need to take a break, take Mr. McInvaille back in the back, have him show us how this all works so that we could cross-examine the detective. So that's problem number one.

And problem number two, I think, is all we need to do is interview Detective Hylton. We've asked for that conversation to happen. I know Mr. Duffey, very, very early on in this case, had suggested that maybe we could do that, and then that discussion fell through, and then here we are.

But I think it matters, as we've talked about, that the crux of this case at this juncture is the motion to suppress.

I did want to, before moving on to the last few points, make sure that when the materials that we're seeking -- one item which we had in small print on our prepared materials Mr. Price accidently left out, in addition to the policies and procedures and the Wi-Fi points and those lists that he had provided. We are seeking also information about the process that Google used to create this anonymous ID that they listed as device ID in column A on the stage 1 and 2 returns.

The device -- as we've indicated, I think, in

some of the briefing, there is some concern that we have that that ID is not necessarily just something that was generated for the purposes of this warrant. Perhaps it's related to or is a number that resides on an individual phone.

If that is the case, then that means that that number is a Google tracking number, that yes, it doesn't have Laura Koenig or someone else's name attached to it, but it is not anonymous in the sense that it cannot be refound. So that's another point that we wanted to make sure we're clear on that's what we're requesting.

I think point number two, as it relates to Google, is that the government, I think, in sum, is availing themselves of this process. And if Google isn't made to provide the information that we are seeking, then we have a limited, ineffective way to be able to test the data, its accuracy, its range, the radius that Google has turned over. And that's why we're seeking, as we've discussed, the access points, the algorithm, or whatever process Google uses to do that.

I think it is important, imperative, for us to remember that unlike some of the other analogies that the government is drawing to other types of

subpoenas or warrants that are served on technology companies like, for example, call detail records, those are business records. Google has stated in its amicus brief that the data that it provided, this is not a business record that Google keeps. Google has to, instead of searching one user's account, search all 1.2 billion of its users is what they proffered. That makes this a very different type of search than the analogies that we have been talking about.

In terms of Mr. Simon's representation that we agree on some things, I think we need to know the details for this Court and any reviewing court, should that become necessary, to be able to work with. Are we talking about a million users? Are we talking about a billion users? Those numbers make a difference. They made a difference to the Court in *Carpenter*, and I anticipate that any future Court, as well as this Court, need to know that information to be able to effectively decide the issues in this case.

Last point, in terms of what Mr. McInvaille had testified about, the location history versus the web activity and the Google location services, he had indicated that the cases that he has worked on where there was an individual user's data sought had come with an indication of the source of that, whether it

was the web activity or the Google location services or location history.

In the geofence data, what I understood him to say is that in the geofence data he has seen in other cases, just as in this case, there is no indication on the spreadsheets that Google provides as to what the source of that data is. That information only comes in the amicus brief, and that's why we're seeking to be able to test that through cross-examination, not simply from a proffer from Google.

Thank you, Your Honor.

THE COURT: All right.

All right. I'm going to get my thoughts together for about ten minutes, and then I'm going to speak to you about my response to your argument.

All right. We'll take a recess.

(Recess taken from 3:30 p.m. until 3:50 p.m.)

THE COURT: All right. Well, clearly, we have in front of us a case of first impression involving technology that both parties, to some degree, are claiming ignorance to and which affects what has been received by the government in a manner that implicates important Fourth Amendment and federal rules issues.

So, here, I have a couple of concerns about what is before me. So, one is your first set of briefing was very good. It did not separate out the standards of materiality under Rule 16 and *Brady*. And it did not separate out how the Court should find whether or not there's a joint investigative team under Rule 16, and, separately, whether Google would be a member of the prosecution team under *Brady*.

So we can't merge those standards because they are different. If they end up being the same, then you have to tell me why. And I do think we have some absence of facts, but the issue, of course, really is how the record I have now affects, first, materiality, and materiality as it pertains in this case looking forward.

So, you all have to do some thinking about how you take a standard that is based on cases that are on habeas usually or appeal, about how it would affect it backward to what happens here as to how it would affect a decision looking forward. It's an importantly different procedural posture.

And just concluding that it would affect materiality needs to be explicated a little bit more under each standard. And you have to use the language that I'm going to have to apply, which is looking

forward, not looking backward, and whether that changes anything. If you don't think it changes anything, then tell me that. And tell me why you don't think it changes anything.

There's note passing. Do you want to say something to me?

MS. KOENIG: No, Your Honor. I was just trying to anticipate where the Court may be going, thinking we will probably want to get a transcript. And I just simply passed a note to say did they want to split the cost of the transcript. I'm sorry that we were note passing.

THE COURT: All right. So, I do want additional briefing. I want it based on the testimony today and the evidence that is currently before the Court. So you probably will need a transcript. You figure out how to pay for it.

And I do think that there is some continued dispute as to exactly what standards apply and how. And I want you to tell me what to do about that before we get into the suppression hearing itself.

So, whatever the government may or may not have any obligation to turn over, the process of narrowing down, I'm just going to tell you there's some practical sense of whether or not Mr. Chatrie is

going to be able to cross-examine that on the fly, whether that's practical, because it's a lot of information.

And so I'm going to ask you to take that into consideration. We can have a two-part hearing. We can do whatever you think is appropriate.

We are in a different procedural posture here, and I do believe that the parties should address some of the things that they disagreed about, some of the things they've agreed about. Certainly I need to know about what the magistrate is just so that's on the record and clear about who that is.

I'm happy to have you all file that by Friday. I think that's a single Westlaw search, and I'm hopeful it can be a joint stipulation. It may or may not matter. I just want to be clear because everybody kept saying "judge."

So I don't know how quickly we can get a transcript.

(Discussion with the court reporter.)

THE COURT: I'll tell you, based on what I have in front of me, this would be my proposed schedule. I would continue with the expert disclosures. I think that's going to help flesh out the record, in any event. And we're going to have a

motion to suppress one way or the other. Is there any objection to that?

MR. SIMON: No objection, Judge.

MS. KOENIG: Not from the defense, Judge.

THE COURT: All right. I think that's going to help you submit your information.

You can speak with the court reporter as to when you will be able to get a transcript, but in any event, you can be planning your arguments with respect to the legal aspects in the meantime.

I'm willing to wait for complete briefs both as to materiality and as to member of the prosecution team or joint investigation until February 18. That gives you plenty of time to address those issues. Obviously, it means we will not have the motion to suppress on the 20th and the 21st.

And I do want you to address the issues that have come up today. Just give me the information that you think I need, and why, and apply the law as I actually have to apply it as far as the standards and as far as the facts.

On the 18th, I would like you to file cross motions as to materiality and as to the joint investigation, including the facts and the standards that have to apply.

Then I want responsive cross motions on the 25th, seven days later. And you all can address whether or not you seek more argument, whether you seek more evidentiary hearing, whatever you want to address in your first motion. And then I will take it under advisement and schedule what I think is appropriate once I have the full record on the 25th.

All right?

MR. SIMON: Yes. Thank you, Judge.

MS. KOENIG: I understand. Thank you.

THE COURT: So I am going to say that I think you all are working hard at this. It is a case of first impression, and it is coming at a weird procedural posture. I think that when we're talking about a warrant that implicates even a million folks who we can presume at least a million minus two of them were definitely not involved in the robbery, we have to be really careful about what we're doing.

And certainly if it's a billion, I think that's something that we really have to be careful about, and I want to be careful about how I find my record. So that either way, I may get it wrong, but I'm going to make as good a record as I can, based on what I have, and you all are helping me do that, but I can't do it just yet. It's a lot of information, and

it's new technology, and I really need to get it right.

So, is there anything else?

MR. SIMON: Judge, are you sufficient -- are we sufficiently good on the Rule 17 piece here? There need not be additional briefing there, right?

THE COURT: I think both parties here acknowledged it was an option; right?

MR. SIMON: Correct, Judge.

THE COURT: I am disinclined to give a party instructions about what to do. Some things seem more straightforward than others, but that's not for me to say. I don't think I can give advice. I don't think I need further briefing because it's certainly an option. And it's an option I think even if Google is a member of the prosecution team. It is a belts-and-suspenders issue. All right? Does that answer your question?

MR. SIMON: Yes, Judge.

THE COURT: Ms. Koenig, do you have any comments or questions?

MS. KOENIG: I do not, Your Honor. Thank you.

THE COURT: All right. Okay. Thank you all for your efforts. I know it was a long day.

(The proceedings were adjourned at 4:00 p.m.)

I, Diane J. Daffron, certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/s/

_____ _____

DIANE J. DAFFRON, RPR, CCR DATE

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

DEFENDANT OKELLO CHATRIE'S SUPPLEMENTAL MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A "GEOFENCE" GENERAL WARRANT

Okello Chatrie, through counsel, submits this supplement to his motion to suppress all evidence and fruits obtained from a "geofence" general warrant, ECF No. 29, pursuant to the Court's Order entered on May 13, 2020. *See* ECF No. 103.

INTRODUCTION

This case turns on a novel and invasive form of electronic surveillance, a so-called "geofence" warrant, involving the search of "numerous tens of millions" of Google users to generate a single investigatory lead. *See* ECF No. 96-1 at 4. Local police had no suspects in the robbery of the Call Federal Credit Union, so they decided to enlist Google to sleuth for them. Investigators went to a Virginia magistrate and, without conveying critical information, obtained a staggeringly broad and unparticularized warrant to go fishing in a pool of private location data that most people have never heard of. They demanded the location information associated with all Google users who happened to be in the vicinity of the bank during rush hour on a Monday evening, and thus, caused Google to search numerous tens of millions of accounts at their behest.

The basic facts involved are found in Mr. Chatrie's initial motion to suppress, *see* ECF No. 29 at 4-7. In short, the warrant followed a three-step process Google developed: "Step One" required Google to search all user accounts and provide "anonymized information" about any

devices in the area during the 30 minutes on either side of the robbery. In response, Google searched every user with "Location History" enabled and estimated that 19 devices were within 150 meters of the bank during that one-hour timeframe. Next, in "Step Two," investigators were to cull the list from Step One, after which Google would produce additional, "anonymized" location information about devices of interest for one hour on either side of the robbery (*i.e.*, two hours total), without geographic restriction. But instead of culling the list, investigators demanded additional information on all 19 devices—multiple times. Google did not comply until investigators identified a subset of nine users for further scrutiny. Finally, at "Step Three," investigators narrowed the list to three devices of interest and obtained de-anonymized information about those Google users. One of the three devices belonged to Mr. Chatrie, who became the government's primary suspect. As the government agrees, *see* 1/21/20 Tr. at 172-73, all of the evidence implicating Mr. Chatrie in this crime emanates from this Google geofence search.

From the beginning, Mr. Chatrie has urged this Court to find that such a warrant is unconstitutional, both categorically and on the facts of this case, because it is fatally overbroad and lacks the particularity required by the Fourth Amendment. *See* ECF No. 29 at 3. Since Mr. Chatrie made his initial motion to suppress, however, Google has filed an *amicus* brief and two affidavits that clarify and magnify the scope of the privacy intrusion worked by the government in this case. *See* ECF Nos. 59-1 & 96. The Court also heard testimony from a digital forensics expert, Spencer McInvaille. *See* 1/21/20 Tr. Mr. Chatrie sought leave to file a supplemental motion and present these new facts to the Court in advance of further testimony and argument, and in support of his motion to suppress all evidence obtained from the geofence warrant, as well as all fruits thereof. The Court granted Mr. Chatrie's request and subsequently extended the filing deadline to May 22, 2020. *See* ECF Nos. 101 & 103.

Mr. Chatrie had a reasonable expectation of privacy in his Google Location History records. As the Supreme Court recently recognized in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), such data is capable of revealing the "privacies of life" and is therefore constitutionally protected. *Id.* at 2214. It can reveal who is inside a home, church, or hotel—all of which are implicated here. The ability to access this Google data grants the government unprecedented surveillance powers, enabling investigators to locate individuals quickly, cheaply, and retroactively. This may be a boon to law enforcement, but it is also a Fourth Amendment search, just as it was in *Carpenter*. *Id* at 2230.

The so-called "third-party doctrine" does not apply to Location History records, and therefore a *valid* warrant—*i.e.*, one that is properly particularized and supported by probable cause—should be required in order for law enforcement to access it.

Location History records are qualitatively different than the "business records" that have fallen into the traditional third-party exception, such as bank deposit slips or telephone numbers dialed. *See United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979); *see also Carpenter*, 138 S. Ct. at 2216–17. As the Supreme Court has recently and repeatedly articulated, digital is different. *See id.* at 2214; *Riley v. California*, 573 U.S. 373, 393 (2014) (comparing a physical search to the search of a cell phone is like "saying a ride on horseback is materially indistinguishable from a flight to the moon"); *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks") (Sotomayor, J., concurring). As a result, any extension of old rules to digital data "has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489.

In this case, Mr. Chatrie did not "voluntarily" convey his cell phone location data to Google in any meaningful way. Like many Google users, he did not knowingly or intentionally "opt-in" to Google's Location History service. And like the cell site location information in *Carpenter*, his Location History data is not subject to the third-party doctrine.

While the government obtained a warrant in this case, it did not obtain one for Mr. Chatrie's Location History data. In fact, it did not seek anyone's data in particular. Rather, the government compelled Google to search *everyone's* data in order to develop an investigative lead. This warrant was unconstitutional. It was both overbroad and lacking in particularly, a forbidden general warrant purporting to authorize a dragnet search of Google users. It did not—and could not—satisfy the Fourth Amendment's probable cause and particularity requirements, rendering it wholly impermissible and void from the beginning. Indeed, it was so deficient that no objectively reasonable officer could rely on it, and as a result, Mr. Chatrie asks this Court to suppress all evidence obtained as a result, as well as all fruits of the poisonous tree.

NEW FACTS

Mr. Chatrie initially characterized the geofence warrant in this case as "a general warrant purporting to authorize a classic dragnet search of every Google user who happened to be near a bank in suburban Richmond during rush hour on a Monday evening." ECF No. 29 at 3. At the time, Mr. Chatrie understood this search to encompass "a trove of private location information belonging to 19 unknown Google users" who were within 150 meters of the bank. *Id.* But that, it turns out, was just the tip of a gargantuan iceberg. As Google now explains, the geofence search involved not just 19 users near the bank, but "roughly one-third of active Google users (i.e., numerous tens of millions of Google users)." ECF No. 96-1 at 3.

Geofence warrants differ from other types of law enforcement requests, entailing a uniquely broad search of all Google users who have "Location History" enabled on their devices. *See* ECF No. 59-1 at 11. Whereas typical requests compel Google to disclose information associated with a specific user, "[g]eofence requests represent a new and increasingly common form of legal process that is not tied to any known person, user, or account." *Id*; *see also* 1/21/20 Tr. at 21. Here, the warrant did not identify Mr. Chatrie in any way. Nor did it identify any of the users whose personal information was searched and turned over to law enforcement. Instead, the warrant operated in reverse: it required Google to identify users with Location History records and then allowed police full discretion to cull through this private information for devices of interest.

Geofence warrants require Google to produce data regarding all Google users who were within a geographic area during a given window of time. But, as Google explains, there is "no way to know ex ante which users may have [Location History] data indicating their potential presence in particular areas at particular times." *Id.* at 12. Thus, in order to comply with the request, Google must "search across all [Location History] journal entries to identify users with potentially responsive data, and then run a computation against every set of coordinates to determine which [Location History] records match the time and space parameters in the warrant." *Id.* at 12-13.

Location History records are one of three types of user location information maintained by Google. If a user has the Google Location History service enabled, then Google estimates the user's device location using GPS signals, signals from nearby Wi-Fi networks, Bluetooth beacons, or cell phone towers. *See* ECF 96-1 at 4. Google saves this information on a map in each user's "Timeline," *id.* at 2, which Google describes as a "digital journal" of a user's locations and travels. *See* ECF No. 59-1 at 16. Google considers this information to be communications "content" for

purposes of the Stored Communications Act, 18 U.S.C. § 2703, requiring the government to obtain a warrant supported by probable cause in order to access it. *See id*.

In addition to Location History records, Google maintains separate databases for user location information derived from two other Google services: "Web & App Activity" and "Google Location Accuracy." Web & App Activity is on by default and it saves location information generated from activities like running a Google Search or using a Google application such as Google Maps, Gmail, or YouTube. *See* ECF No. 96-1 at 5; 1/21/20 Tr. at 23; *In Re Google Location History Litigation*, No. 5:18-cv-05062-EJD (N.D. Cal. Dec. 19, 2019). Google uses this data to provide "a more personalized experience" through "faster searches and more helpful app and content recommendations." ECF No. 96-1 at 5. Google asserts that it did not search the Web & App Activity database in this case because that database does "not store a user's location at a level of detail precise enough to be responsive to a geofence warrant."[1]

Google Location Accuracy, formerly known as "Google Location Services," works on Android devices and is also enabled by default. It estimates a device's location using GPS data, Wi-Fi access points, Bluetooth sensors, and mobile network information. *See* ECF No. 96-1 at 6; 1/21/20 Tr. at 23. Google uses this information to improve location accuracy by estimating the physical location of Wi-Fi access points, Bluetooth beacons, and cell phone towers based on the GPS coordinates transmitted by devices that interact with those networks. *See* ECF No. 96-1 at 6-7; 1/21/20 Tr. at 64-65. "In other words," explains Google, "[Google Location Accuracy] data might be used by the device to calculate a location data point that is stored in [Location History.]"

[1] Google states that Web & App Activity data "reflects a device's location to an approximate area of at least one square kilometer" and is "therefore too coarse to be responsive to the warrant," which initially entailed a search area with a 150-meter radius. ECF No. 96-1 at 8.

Id. at 6.[2] Google asserts, however, that it did not directly search the Google Location Accuracy database in response to the geofence warrant because the data is "not stored with user identifiers" and is "used in an anonymous way." *Id.*

Thus, even though the geofence warrant required Google to produce location data for "each type" of Google account inside the geofence, *see* ECF No. 54-1 at 4, 9, Google did not do so. Instead, Google says that it only searched the Location History database, not the Web & App Activity or Google Location Accuracy databases. *See* ECF No. 59-1 at 12; ECF No. 96-1 at 7-8. According to Google, Location History is the only form of data that is "sufficiently granular" and searchable to be responsive to a geofence request. ECF No. 96-1 at 7.

Consequently, Google did not search the contents of every Google user in order to respond to the warrant. Instead, it searched those users with Location History enabled on their accounts—*i.e.*, the "Sensorvault." But this is no small number. It amounts to "roughly one-third of active Google users." *Id.* at 4. Not even Google, however, knows precisely how many users it searched in this case. *Id.* Rather, Google estimates that "numerous tens of millions of Google users" had Location History enabled in 2019, all of whom had their accounts searched in order to identify 19 users who were, perhaps, roughly within 150 meters of the bank. *Id.*[3]

Of critical importance is that, in practice, the effective range of the geofence was more than double 150 meters. As a result, at least some of the 19 users identified by Google were likely never within the 150-meter geofence at all. As Google states, "it is possible that when Google is

[2] When estimating a user's location through the Location History service, Google appears to use historical location data from other users, stored in the Google Location Accuracy database, to estimate a device's likely GPS coordinates based on the presence and strength of known nearby Wi-Fi, Bluetooth, and cell phone tower signals. For example, if many devices transmit a similar set of GPS coordinates when they "see" a particular Wi-Fi network, then Google may attribute those GPS coordinates to a device that later "sees" the same Wi-Fi network if GPS is unavailable for that device.

[3] Thus, assuming Google has two billion active users, a third of which is 660 million (*i.e.*, twice the population of the United States), then 19 users represent a hit rate of 0.0000029%.

compelled to return data in response to a geofence request, some of the users whose locations are estimated to be within the radius described in the warrant (and whose data is therefore induced in a data production) were in fact located outside the radius." *Id.* at 9; *see also* ECF No. 59-1 at 20 n.12 (estimates may include "false positives—that is, that [they] will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there."); 1/21/20 Tr. at 65. This phenomenon is a product of how Google calculates a user's location based on "multiple inputs," including the strength of nearby Wi-Fi signals. ECF No. 96-1 at 8; *see also supra* n.2. According to Google, the latitude/longitude coordinates saved in Location History records do not necessarily reflect a user's actual location, *id.*, but are "probabilistic estimates," each with a different "margin of error." ECF No. 59-1 at 10 n.7. Google presents that margin of error as a "Map Display Radius," which is often depicted on a map as a shaded blue circle extending outwards from the "blue dot" indicating the user's estimated location. ECF No. 96-1 at 9. Importantly, there is only an "estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot." *Id.* Or in other words, chances are better than 1-in-5 that the user is outside of the shaded circle altogether.[4]

Google has provided numerical values for the margins of error in this case, the largest of which is 387 meters from coordinates near the center of the 150-meter geofence. *See* ECF No. 68 Ex. A at 6-12, 17-37. Figure 1, below, depicts the 150-meter geofence in red and the 387-meter margin of error in yellow. That margin of error indicates that at least one user[5] could have been more than 387 meters away from the bank—and more than 237 meters outside the geofence—but

[4] The size of the margin of error depends on the user location data available to Google. For example, coordinates obtained from GPS signals are more accurate than coordinates derived from Wi-Fi signals. *See* 1/21/20 Tr. at 64. In this case, 88% of the coordinates at issue were derived from Wi-Fi signals, as opposed to GPS. *Id.* None were derived from Bluetooth or cell phone tower data.
[5] "Device ID" number 702354289.

was nonetheless swept into the dragnet. In fact, Google is only 68% confident that the user was not even farther away than 387 meters. Put it another way, the yellow line indicates the minimum effective range of the geofence in this case, which is more than twice what the warrant authorized.



Figure 1

The true reach of the geofence, therefore, included not only a major thoroughfare (U.S. Route 360), the bank, and the Journey Christian Church, but also another road next to the church, a Ruby Tuesday restaurant, a Hampton Inn hotel, a mini storage facility, an apartment complex for seniors, and another residential apartment complex. *See* Tr. 1/21/20 at 66-67. Numerically, the 150-meter radius covered an area of 78,000 square meters, or about 17 acres, whereas the effective range was 470,000 square meters, or about 116 acres—an increase of more than 500 percent.

ARGUMENT

Execution of the geofence warrant was an unconstitutional search that intruded upon Mr. Chatrie's reasonable expectation of privacy in his Google location data. As Mr. Chatrie contends, the warrant was invalid because it was a general warrant, fatally overbroad and devoid of particularity, and therefore impermissible under the Fourth Amendment. *See* ECF No. 29 at 7, 16-24. Moreover, the warrant was *void ab initio*—so obviously deficient from the beginning that the search must be regarded as warrantless. As a result, the good-faith doctrine does not apply and the results of the search, including all of its fruits, should be suppressed.

I. The Geofence Warrant Intruded on Mr. Chatrie's Reasonable Expectation of Privacy in His Location History Records.

As Mr. Chatrie argues in his initial motion to suppress, the Supreme Court's recent decision in *Carpenter* applies to mobile location data obtained from Google just as much as similar data obtained from a cellular service provider. *See* 138 S. Ct. 22; ECF No. 29 at 7-11. Narrowly construed, *Carpenter* found a reasonable expectation of privacy in seven days of historical cell-site location information ("CSLI"), *id*. at 2217, because seven days was the shortest amount of time on the record before the Court. *See* ECF No. 48 at 2-4. Nonetheless, *Carpenter's* reasoning applies with at least equal force here. As Justice Gorsuch noted in dissent, presciently: "[W]hat distinguishes historical data from real-time data, or seven days of a single person's data from a download of *everyone*'s data over some indefinite period of time? . . . On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not?" *Id.* at 2267 (emphasis in original). The government struggles to argue that technical differences compel a different conclusion here, but Justice Gorsuch is correct. There are no principled distinctions to be had.

The government's primary objection centers on the length of the search, which covered two hours during rush hour on a Monday evening in Richmond, as opposed to the seven days at issue in *Carpenter*. But by "declin[ing] to determine whether there is a 'limited period' for which the government can acquire cell phone location information without implicating the Fourth Amendment," ECF No. 41 at 7, the Supreme Court did not give the government a free pass to obtain less than seven days of location data without a warrant. (In fact, the government's demand for seven days of data in *Carpenter* netted only two days of data. *See* 138 S. Ct. at 2212.)

On the contrary, the Supreme Court has repeatedly expressed concern that even short-term location tracking may constitute a search. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *accord Carpenter*, 138 S. Ct. at 2215. Indeed, there are significant privacy implications involved in just a single trip to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-442 (2009)). And this is especially true where the search reveals information about the interior of a constitutionally-protected space, such as a home. *See United States v. Karo*, 468 U.S. 705, 716 (1984) (finding that the use of a beeper to track a drum of chemicals into a private residence was a search); *see also Kyllo v. United States*, 533 U.S. 27, 37 ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."). Such intrusions are "presumptively unreasonable in the absence of a search warrant." *Katz v. United States*, 389 U.S. 347, 361 (1967); *Kyllo*, 533 U.S. at 31 ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'") (quoting *Silverman v. United States*, 365 U.S. 505 (1961)).

In this case, the geofence search revealed Google users who were not only inside the bank, but also in nearby homes, apartment complexes, and, it would seem, the Journey Christian Church. *See* 1/21/20 Tr. at 80-82 (describing the data for "Mr. Green," which begins at a hospital, ends at a private residence, and incorrectly indicates he went into church); *id.* at 83-85 (describing the data for "Mr. Blue," which shows a trip to a private residence with start and end points in an apartment complex); *id.* at 88-90 (describing the data for "Ms. Yellow," which shows a trip from a single-family residence to Manchester High School, followed by two local businesses, and then a return trip home). While this data was supposedly "anonymized" by Google, the defense was able to ascertain the likely identities of Mr. Green, Mr. Blue, and Ms. Yellow based upon the addresses of the residences involved, their travel history, and other publicly available information. *See id.* at 83, 87-88, 90-91.

Google's handling of the data at issue lends further credence to the notion that any slice of Location History data is private, no matter how small. Google considers Location History to be communications "contents" for purposes of the Stored Communications Act, 18 U.S.C. § 2703, meaning that from a privacy perspective, it is on par with the contents of an email or personal documents stored remotely on Google Drive. *See* ECF No. 59-1 at 9, 17; ECF No. 72 at 3. Far from an ordinary "business record," Google considers Location History to be a "digital journal" of users' movements and travels. ECF No. 59-1 at 16. As a result, Google requires the government to obtain a warrant supported by probable cause in order to access Location History records. *Id.* at 15-18. There is no exception for two hours of private, invasive data.

Finally, Location History records are at least as accurate as the cell site location information ("CSLI") in *Carpenter*, and equally capable of revealing the "privacies of life." 138 S. Ct. at 2217. Initially, Mr. Chatrie argued that all of the records in this case were "more precise than the cell site

location at issue in *Carpenter*." ECF No. 29 at 12. But as Google's *amicus* brief makes clear, Google derives Location History coordinates from "multiple inputs," some of which are more accurate than CSLI and some of which are not. ECF 96-1 at 4. These "inputs" include GPS signals, which are highly accurate and can estimate a device's location within "approximately twenty meters or less." *Id*. But they may also include Wi-Fi, Bluetooth, and CSLI data, which is generally less accurate than GPS. *Id*. Google explains that "[c]ombined, these inputs . . . can be capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI." *Id*.[6]

Nonetheless, Location History is at least as accurate as CSLI, *i.e.*, the least accurate "input" that Google uses. Furthermore, the *Carpenter* Court equated CSLI and GPS for purposes of Fourth Amendment analysis. *See* 138 S. Ct. at 2217 ("As with GPS information, the time-stamped [CSLI] data provides an intimate window into a person's life, revealing . . . his particular movements") (internal citation omitted). And as *Carpenter* instructs, courts should anticipate advances in the accuracy of such technologies in order to "'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" 138 S. Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) (alteration in original); *accord United States v. Jones*, 565 U.S. 400, 406 (2012). When new technologies "encroach upon areas normally guarded from inquisitive eyes," *id.*, courts must remain vigilant "to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Id.* at 2223. Indeed, not even the government finds a meaningful difference between CSLI and GPS, conceding that *Carpenter* "t[ook] account of

[6] At the same time, however, because Location History was developed for the purpose of targeting customer advertisements and not for impeccable surveillance, estimates based on CSLI or Wi-Fi signals may be far less accurate than estimates based on GPS tracking. Consequently, a geofence search may mistakenly identify some users as being within the radius who were in fact located outside of it. *Id.* at 9. In the case, Google appears to have identified at least one user inside the Journey Christian Church who was likely never in the church at all, and may in fact have been more than 387 meters away. *See supra* at 9-10.

more sophisticated systems" and recognized that CSLI "is rapidly approaching GPS-level precision." ECF No. 41 at 8.

In this case, the Location History records produced by Google involve a mix of GPS and Wi-Fi inputs, with approximately 12% coming from GPS and 88% coming from Wi-Fi signals. *See* 1/21/20 Tr. at 64. But the government did not and could not—because of the nature of the colossal search Google conducts in these types of cases—know in advance which sources of location data would ultimately be at issue. Rather, because GPS and CSLI are among the potential sources, the analytical assumption has to be that Location History records may be least as precise as the GPS or cell site signals in *Jones* and *Carpenter*.

II. The Third-Party Doctrine Does Not Diminish Mr. Chatrie's Expectation of Privacy in His Google Location Data.

The third-party doctrine does not apply to Location History records or diminish Mr. Chatrie's privacy interest in them. The doctrine generally holds that individuals do not have a reasonable expectation of privacy in information "voluntarily" conveyed to a third-party, but the *Carpenter* Court was clear that the rule is not to be "mechanically" applied in the digital age. 138 S. Ct. at 2219; *see also* ECF No. 29 at 9-11. Instead, *Carpenter* teaches that mobile location information is a "qualitatively different category" of data, distinct from the telephone numbers and bank records in *Miller*, 425 U.S. 435, or *Smith*, 442 U.S. 735. *See* 138 S. Ct. at 2216–17. The same reasoning applies here.

As Mr. Chatrie argues, "Google location records are qualitatively different from the business records to which the third-party doctrine traditionally applies." ECF No. 29 at 9. Unlike the numbers dialed in *Smith* or the bank deposit slips in *Miller*, Location History records are "detailed, encyclopedic, and effortlessly compiled," *Carpenter*, 138 S. Ct. at 2216, as well as deeply revealing. *See* ECF No. 29 at 12-13. Granting the government access to this information is

an unprecedented new surveillance power, akin to handing it a time machine capable of locating Google users in the past, all without expending finite physical resources like manpower or unmarked cars. *See id*. at 13-14. In short, it "gives police access to a category of information otherwise unknowable." *Carpenter*, 138 S. Ct. at 2218; *see also Prince Jones v. United States*, 168 A.3d 703, 714 (D.C. 2017) (use of a "cell site simulator" to locate a person through a cell phone is a search because the information is not readily available or in the public view, unlike visual surveillance or older generations of tracking devices).

The government counters that Mr. Chatrie has "voluntarily" shared this data with Google because Location History is an "opt-in service." *See* ECF No. 41 at 10-12. Google also describes "several steps" that a user must take in order for Location History to function and save information. ECF 96-1 at 2-3; ECF 59-1 at 12. But a closer look at this "opt-in" process reveals that it is not nearly as informed or voluntary as Google and the government suggest. On the contrary, users may unknowingly enable the function without ever seeing the phrase "Location History" or being informed of the privacy implications of turning it on. *See* ECF No. 72 at 6-9; 1/21/20 Tr. at 56-57.

Following the standard setup of an Android phone like the one used by Mr. Chatrie, a user encounters a pop-up screen, reproduced in *Figure 2*, when opening the Google Maps application for the first time. *See* ECF No. 72 at 7; 1/21/20 Tr. at 56. It says, "Get the most from Google Maps" and then it gives the user two options: "YES I'M IN" or "SKIP." *Id.* There is also a statement that reads "Google needs to periodically store your location to improve route recommendations, search suggestions, and more" and a button to "LEARN MORE." ECF No. 72 at 7. The pop-up does not use the phase "Location History," but clicking on "YES I'M IN" enables the function. Clicking on "LEARN MORE" takes the user to a webpage with Google's complete Privacy Policy and Terms

of Service; it does not direct the user to any specific language concerning location data or Location History specifically. *See* 1/21/20 Tr. at 57.

In fact, Google's Terms of Service do not mention Location History at all. *See* Google, Terms of Service (Oct. 25, 2017).[7] And Google's Privacy Policy, which is 27 pages long, mentions Location History only twice. *See* Google, Privacy Policy at 4, 8 (Jan. 22, 2019).[8] In the first

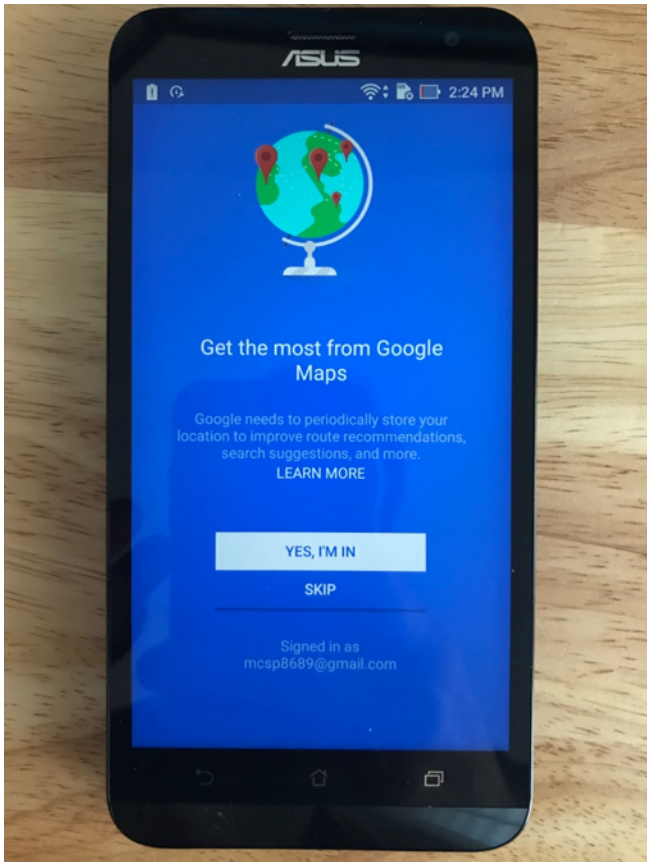


Figure 2

instance, it says, in full: "You can also turn on Location History if you want to create a private map of where you go with your signed-in devices." *Id.* at 4.[9] If anything, the phrase "private map"

[7] *Available at* https://policies.google.com/terms/archive/20171025.
[8] *Available at* https://www.gstatic.com/policies/privacy/pdf/20190122/f3294e95/google_privacy_policy_en.pdf.
[9] The Privacy Policy links to a current webpage with instructions on how to "Manage your Location History." The only date on the webpage is 2020 and it is not clear whether or what version of this page existed at the time Mr. Chatrie set up his phone.

is misleading and suggests that Google does not have access to the data. In the second instance, the policy says, in full: "Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions." *Id*. at 8. Of course, "traffic predictions" do not begin to suggest that Google will keep a 24/7 "journal" of a user's whereabouts. But even if it did, a user would have no way of knowing that the pop-up "opt-in" screen relates to the Location History feature.

The pop-up does not reference "Location History" by name. As a result, a typical user would not know to scour Google's policies for references to Location History, much less understand the implications of the choice Google is asking them to make. In short, it is strikingly easy for a user to "opt-in" to Location History without ever being aware of doing so.

Consumer groups across Europe have filed complaints against Google over its location data practices, citing the deceptive design of the Location History "opt-in" process. *See Groups Across Europe File Complaints Against Google for Breach of GDPR*, The European Consumer Organisation (Nov. 27, 2018).[10] A complaint from Norway, for example, alleges that user consent to Location History tracking is not valid because it is not "freely given," "specific and informed," or "unambiguous." *Complaint to the Datatilsynet Under Article 77(1) of the European General Data Protection Regulation* at 8-12, Forbrukerrådet (Nov. 27, 2018).[11] Specifically, it argues that Location History can "be easily turned on involuntarily" and that the "relevant information regarding what Location History actually entails is hidden behind extra clicks and submenus, and the information about what the data is used for is ambiguous and unclear." *Id*. at 3, 11. It also

[10] *Available at* https://www.beuc.eu/publications/consumer-groups-across-europe-file-complaints-against-google-breach-gdpr/html.
[11] *Available at* https://fil.forbrukerradet.no/wp-content/uploads/2018/11/complaint-google-27-november-2018-final.pdf.

alleges that Google uses pop-up consent screens for Location History, similar to the one in Google Maps, in conjunction with other Google applications such as Google Assistant, the Google Search app, and Google Photos. *Id.* at 9. The cumulative effect is that a "user is repeatedly compelled to give consent using design patterns and biased notices," thereby increasing the likelihood that the user will "opt-in" by accident, out of frustration, or because of a belief that the services will not work otherwise. *Id*. In sum, "due to the deceptive design used by Google, it is not entirely clear for the user that she is actually giving consent to something, and even it was, it is not exactly clear to what she is consenting." *Id*. at 12; *see also Every Step You Take* at 16-23, Forbrukerrådet (Nov. 27, 2018) (the report on which the European complaints were based).[12]

On this side of the Atlantic, courts have been skeptical of so-called "clickwrap" contracts of adhesion. *See, e.g., Nguyen v. Barnes & Noble*, 763 F.3d 1171, 1175-76 (9th Cir. 2014) (categorizing "[c]ontracts formed on the Internet" as "clickwrap" or "browsewrap" depending on how they provide notice and seek assent); *Berkson v. Gogo*, 97 F. Supp. 3d 359, 395-401 (E.D.N.Y. 2015) (discussing "browsewrap," "clickwrap," "scrollwrap," and "sign-in-wrap"). Although the Fourth Circuit has not yet weighed in,[13] a recent opinion from this district is instructive. *See Melo v. Zumper*, No. 3:19-cv-621 (DJN), 2020 WL 465033, at *8-11 (E.D. Va. Jan. 28, 2020).

Like this case, *Zumper* involved a pop-up consent screen, but that is where the similarities end. The crucial question for the court in *Zumper* was "whether the website presented the terms

[12] *Available at* https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf. The study's tests were performed "using a Samsung Galaxy S7 Android device running Android version 8.0.0" and then reproduced on a "Google Pixel device running Android 9." *Id.* at 6. While the "settings and device setup process may vary somewhat between devices," the results were "representative of a typical user experience." *Id*.; *see also* 1/21/20 Tr. at 36-37, 45-48 (discussing similarities in Location History prompts between Android versions).

[13] The Fourth Circuit in *A.V. ex rel. Vanderhye v. iParadigms*, LLC, 562 F.3d 630, 645 n.8 (4th Cir. 2009), "decline[d] to address the question of whether the terms of the Clickwrap Agreement created an enforceable contract."

and conditions in a hyperlink, and whether that hyperlink appeared clearly to the user." *Id.* at *9. In making this determination, the court considered the "placement of the terms and conditions hyperlink in relation to the button that grants a user access," "whether the terms and conditions hyperlink appeared to the user on multiple occasions," and "the overall design elements of the website, including font size and color, and other visual components that might hinder a user's reasonable notice." *Id.* at *9-10. In *Zumper*, the court concluded that the interface did provide sufficient notice of the company's terms and conditions because the company included a warning that "clearly stated that 'by creating a Zumper Account you indicate your acceptance of our Terms and Conditions and Privacy Policy," which were accessible through a conspicuous hyperlink directly below the "Create Account" button. *Id.* at *10-11.

In this case, by contrast, the "design and content" of Google's interface objectively obfuscates and discourages users from understanding what they are agreeing to. *See Berkson*, 97 F. Supp. 3d at 401. The pop-up here focused the user's attention on "get[ting] the most out of Google Maps" and did not mention Location History at all, let alone explain what clicking "YES, I'M IN" would entail. *See* Figure 2, *supra*; 1/21/20 Tr. at 56.

Mr. Chatrie would have had to agree to Google's terms and conditions during the initial setup process of his phone. *See* 1/21/20 Tr. at 50. But unlike the pop-up in *Zumper*, he did not have to view or assent to the terms again when he encountered the pop-up "opt-in" screen. He was not required to click through the text of Google's terms before Location History collection began; a renewed reference to the terms was not displayed, prominently or otherwise. *Cf. Tradecomet.com v. Google*, 693 F. Supp. 2d 370, 377-78 (S.D.N.Y. Mar. 5, 2010) (clickwrap agreement was reasonably communicated where the user "had to click through the text of that agreement" in order to agree"); *Moore v. Microsoft Corp.*, 293 A.D.2d 587, 587 (N.Y. 2002) (finding assent where the

terms were "prominently displayed on the program user's computer screen before the software could be installed" and the user was required to "click[] on the 'I agree' icon before proceeding with the download of the software."); *Feldman v. Google, Inc.*, 513 F. Supp. 2d 229, 237 (E.D. Pa. 2007) (finding notice and assent where "the user had to visit a webpage which displayed the Agreement in a scrollable text box," there was a "prominent admonition in boldface to read the terms and conditions carefully," and the terms were "only seven paragraphs long—not so long so as to render scrolling down to view all of the terms inconvenient or impossible"). The prompt did not even use the words "I Agree" or "Terms and Conditions," which may have at least implied that users were giving up something. *See* 1/21/20 Tr. at 56-57.

A "LEARN MORE" button is no substitute for a clear statement that users are agreeing to something drastically new. After all, the initial setup process—the point at which Mr. Chatrie did have to accept Google's terms—indicates that Location History is *not enabled* by default. *See* 1/21/20 Tr. at 53. Nothing about the pop-up screen indicates that users would be reasonably informed that they are changing this default setting or opting-in to the Location History service. Providing a link to all of Google's policies and terms of service is meaningless without a clear indication of what is changing and where to look.

III. The Geofence Warrant Infringed on Mr. Chatrie's Property Interests in His Location History Records and Was Therefore a Fourth Amendment Search.

Mr. Chatrie reiterates that he has a property interest in his Location History records, which constitute his private "papers and effects." *See* ECF No. 29 at 14-16; ECF No. 48 at 8-10. Google is a mere bailee of these records and the government can only search and seize them with a valid warrant. *See* ECF No. 29 at 15-16. The government has yet to address the substance of this argument, dismissing it as a theory "rooted in Justice Gorsuch's solo dissent in *Carpenter*," ECF No. 41 at 12. The government simply does not engage with centuries of Supreme Court

jurisprudence that embraces—and continues to validate—a property-based understanding of the Fourth Amendment. *See* ECF No. 48 at 8-10; *Carpenter*, 138 S. Ct. at 2213-2214 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection"); *Jones*, 565 U.S. at 406-07 ("For most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding."); *id.* at414 ("*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.") (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 40 ("well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass").

Mr. Chatrie fully adopts, incorporates, and re-asserts his property-based arguments here. *See* ECF No. 29 at 14-16; ECF No. 48 at 8-10. If anything, Google's repeated insistence that Location History data is a personal "journal" only solidifies this claim, even if it is not a journal that users know they are keeping. *See* ECF No. 59-1 at 16; ECF No. 96-1 at 9. Regardless of whether the Court analyzes Mr. Chatrie's claim under a property-based theory or the reasonable expectation of privacy framework set forth in *Katz*, the result is the same. The search of Mr. Chatrie's Google Location History records was a Fourth Amendment search.

IV. The Geofence Warrant Was an Unconstitutional General Warrant, Fatally Overbroad and Lacking Particularity.

Mr. Chatrie also renews his argument that geofence warrants are inherently unconstitutional. They are the epitome of the indiscriminate, "dragnet"-style searches that the Supreme Court has repeatedly warned against—and that the Framers fought a revolution to prevent. *See* ECF No. 29 at 16-23. Indeed, the Supreme Court has never upheld anything remotely approaching the search of "numerous tens of millions" of people. *See* ECF No. 96-1 at 4. The new facts presented by Google in its *amicus* brief and affidavits only confirm that the warrant in this

case was uniquely overbroad and so lacking in particularity that it can only be described as the digital equivalent of an impermissible general warrant.

A. Overbreadth

The geofence warrant here did not—and could not—meet the probable cause or particularity requirements demanded by the Fourth Amendment. It did not identify any individuals or accounts to be searched because investigators did not know who they were searching for, or even if Google would have relevant data. *See* ECF No. 29 at 23. Nothing in the warrant application indicates that the bank robber was a Google user or had Location History enabled at the time of the robbery. *Id*. Instead, the application rested on broad conjecture based on the popularity of Google and cell phones generally. *See* ECF No. 29 at 23; ECF No. 48 at 19.

From the outset, the government enlisted Google to search untold *millions* of unknown accounts in one of the largest fishing expeditions in Fourth Amendment history. The number of individuals affected by this case dwarfs the number of people searched in any other reported criminal opinion. Even controversial "tower dumps," which are exceedingly broad in their own right, tend to impact hundreds or thousands of people at most. *See, e.g., United States v. James*, No. 18-CR-216, 2019 WL 325231, at *3 (D. Minn. Jan. 25, 2019) ("hundreds if not thousands" of cell phone users); *In re Cell Tower Records Under 18 U.S.C. 2703(D)*, 90 F. Supp. 3d 673, 676 (S.D. Tex. 2015) ("several thousand phone numbers"); *United States v. Pembrook*, 119 F. Supp. 3d 577, 586 (E.D. Mich. 2015) ("potentially hundreds"); *In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d)*, 42 F. Supp. 3d 511, 513 (S.D.N.Y. 2014) ("hundreds or thousands"); *In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 770 (S.D. Tex. 2013) **("**hundreds, or even thousands").

A tower dump requires cell phone service providers to produce the records of every device connected to a particular cell tower or towers during a particular time. *See* ECF 59-1 at 14. But as a practical matter, the number of people affected is limited by the number of cell phone users who were present at the time—*i.e.*, hundreds or thousands, depending on the area and the time. The difference with geofence searches is that there is no such practical upper limit. Rather, Google asserts that it has "no way to identify which of its users were present in the area of interest without searching the [Location History] information stored by every Google user." *Id*. Consequently, the number of users searched using a geofence warrant is bound only by the number of Google users with Location History enabled, which Google estimates to be in the "numerous tens of millions." ECF No. 96-1 at 4.

The government cites to the "Playpen" cases as a justification for the breadth of the search here. *See* ECF No. 41 at 19-20. Those cases arose from a warrant that searched users who logged into a child pornography website temporarily run by the FBI. The scheme was one of the largest sting operations in history, but it still only involved "approximately nine thousand" computers globally. *See* Order on Defendants' Motion to Dismiss Indictment at 5, 12, *United States v. Tippens*, No. 16-05110-RJB (W.D. Wash. Nov. 30, 2016) (ECF No. 106). Moreover, users had to take numerous affirmative steps to access and log into the website, making it "extremely unlikely for someone to stumble innocently upon Playpen." *United States v. Matish*, 193 F. Supp. 3d 585, 603 (E.D. Va. 2016); *see also United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018) (noting that in order to access Playpen, a user must download special software and enter a 16-character URL consisting of random letters and numbers, as well as enter a username and password to proceed past a welcome page that "was suggestive enough that Playpen's content would be apparent" to any visitor). By contrast, there was no government honeypot in this case, and there is

no argument that using Location History or being near the Call Federal Credit Union is inherently suspicious. *See* ECF No. 48 at 13.

The fact that Google produced the records belonging to 19 of these users does not diminish the scope of the initial search conducted at the government's behest. Unlike scenarios where a company must search defined records to identify responsive data, the search here did not identify any specific users or accounts to be searched. Instead, the warrant forced Google to act as an adjunct detective, scouring the accounts of numerous tens of millions of users with Location History enabled in order to generate a lead for the government. That the intimate, private data of numerous tens of millions of users were searched is the heart of the overbreadth analysis in this case. That records belonging to 19 people were ultimately produced does not lessen the massive, and illegal, search conducted in this case.

B. Particularity

A geofence warrant is overbroad by design, but it is also severely lacking in particularity. Apart from probable cause, the Fourth Amendment requires that warrants "particularly describ[e]" the place to be searched and the things to be seized. U.S. Const. amend. IV. The idea is to leave nothing to the discretion of the officers executing a warrant that a court has properly authorized. *See Marron v. United States*, 275 U.S. 192, 196 (1927). This is especially critical where, as here, a search implicates First Amendment concerns. *See* ECF No. 29 at 13, 22; ECF No. 48 at 3 n.3. If particularized, it should be obvious to all what officers can search and what they can seize. The exact opposite occurred here.

The geofence warrant left it up to Google and the government to negotiate which users would have their account information searched and further revealed to investigators—the hallmark of an unparticularized warrant. *See Steagald v. United States*, 451 U.S. 204, 220 (1981); *Stanford*

v. Texas, 379 U.S. 476, 482-83 (1965) (describing the "battle for individual liberty and privacy" as finally won when British courts stopped the "roving commissions" given authority to "search where they pleased"). As Mr. Chatrie contends, "a three-step, back-and-forth process with the recipient of a warrant is not a substitute for particularizing that warrant at the outset. Instead, it is an unconstitutional delegation of discretion to the executing officers." ECF No. 29 at 23. At each step along the way, Google and the government—not the issuing magistrate—decided what data to search and what data to produce. Even the government now appears to agree that there was some "lack of clarity about what this search warrants asks for." 1/21/20 Tr. at 171.

At Step One, Google made critical decisions that would ordinarily be made by a judge, not the recipient of the warrant. First, Google decided to search only a portion of its records, specifically "Location History" records kept in the "Sensorvault." *See* ECF No 96-1 at 3. Google then decided to ignore the margins of error generated by its own calculations and "estimate" that 19 Google users were within the 150-meter geofence. In reality, at least five of those 19 users were never within the geofence at all.[14] Instead, Google guessed—inaccurately. One device could have been more than 387 meters away from the bank, and yet Google still identified its user as a potential suspect subject to additional search in Step Two.

During Step Two, the warrant said the government would "attempt" to narrow the Step One returns and then obtain additional location information on a subset of devices of interest. *See* ECF No. 54-1, Attach. I at 1-2; Attach. II at 2-3. The government did not try very hard. Instead, the government approached Google multiple times to press for expanded data on all 19 of the devices identified in Step One. First, Detective Hylton emailed Google on or about July 2, 2019, to request "additional location data (*i.e.*, step 2) and subscriber information (*i.e.*, step 3) for all 19

[14] Device IDs 702354289, -965610516, 907512662, 1135979718, and 2021066118.

device numbers produced in step 1." ECF No. 96-2 at 5; *see also* ECF No. 48 at 14, Ex. A at 1. On July 8, Det. Hylton called Google twice, and left two voicemails, presumably requesting the same. *Id.* A Google representative called Det. Hylton back and "explained the issues in the Detective's email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant." *Id.* Google also "explained the importance of step 2 in narrowing" to Det. Hylton. *Id.* At some point, the government emailed Google once again to ask for "additional location data and subscriber info" on all 19 devices identified in Step One. *See* ECF No. 48, Ex. B at 1.[15] In each email, Det. Hylton wrote to Google that, "If this request seems unreasonable, please keep in mind that device numbers 1-9 may fit the more likely profile of parties involved," but proceeded to request additional information on all 19 users anyway. *See* ECF No. 48, Ex. A at 1; *id.*, Ex. B at 1. Eventually, Det. Hylton acquiesced and emailed Google a third time to request additional information on 9 of the 19 users. *Id.*, Ex. C at 1. The third time around, Google complied.

The haggling between Google and Det. Hylton is emblematic of the absence of particularity in the geofence warrant. The Fourth Amendment demands that a neutral and detached magistrate make decisions about what to search and what to seize. This constitutional function cannot be outsourced to Google or to the police. As well-intentioned as Google may be, it is not up to Silicon Valley to determine what is "reasonable." *Cf.* ECF No. 48, Ex. A at 1; *id.*, Ex. B at 1 ("If this request seems unreasonable…"). That decision belongs to the judicial branch, and the judicial branch only. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004) ("Even though [law enforcement] acted with restraint in conducting the search, 'the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.'") (quoting *Katz*, 389 U.S. at 356).

[15] The government has not provided the dates for either of the emails to Google.

Furthermore, a basic premise of the warrant was that the data returns in Step One and Step Two would be "anonymized." But as Mr. Chatrie has consistently argued, "[t]he fact that Google masks the true 'Device ID' with a pseudonym does not make the data anonymous." *See* ECF No. 68 at 3; ECF No. 72 at 10; 1/21/20 Tr. at 83, 87-88, 90-91. On the contrary, every person takes a "unique path through life" that is "inherently identifiable." ECF No. 68 at 3; *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1716 (2010). And as Mr. Chatrie demonstrated, the impossibility of anonymizing location data holds true in this case as well. *See* 1/21/20 Tr. at 83, 87-88, 90-91. It is trivial to plot "anonymized" coordinates on a map, connect the dots, and determine which house belongs to whom. *See* ECF No. 68 at 3; 1/21/20 Tr. at 74-75. Indeed, the Step One returns may be enough, without anything more from Google, for law enforcement to determine the identity of "anonymized" users. *See* 1/21/20 Tr. at 86-87.[16] Consequently, this Court "should not discount the intrusiveness of the initial data returns disclosed by Google." ECF No. 72 at 10.

In Step Three, the government selected three Google users for even further scrutiny. At least one of these users[17] was likely never inside the geofence at all, something which should have been apparent to investigators reviewing the Step Two returns. Nonetheless, the government decided to have Google de-anonymize this user's records and turn over additional subscriber information associated with the account.

[16] For this reason, Mr. Chatrie does not believe it is appropriate, as the government suggests, to sever the warrant and consider Step One separately from Step Two. *See* ECF No. 41 at 20. Furthermore, doing so would "condone the digital equivalent of a general warrant that lacked particularity from the outset." ECF No. 48 at 14 n.5; *see also United States v. Sells*, 463 F.3d 1148, 1158 (10th Cir. 2006) (noting that "every court to adopt the severance doctrine has further limited its application to prohibit severance from saving a warrant that has been rendered a general warrant by nature of its invalid portions despite containing some valid portion").

[17] Device ID: 907512662.

At no point during this three-step process did the government return to the magistrate to seek further authorization. *See* ECF No. 29 at 23-24. Instead, it was up to Google to determine what was "reasonable," beginning with the scope of the initial search, and including the returns provided in Steps Two and Three. ECF No. 48, Ex. A at 1; *id.*, Ex. B at 1. The point is not that Google should have searched the Location Accuracy or Web & App Activity databases, or that Google should have produced more or less records. The point is that this is not how warrants are supposed to work. What the government can search and seize is a question that the Constitution reserves for the judiciary, not for Google or the police. *See Groh*, 540 U.S. at 561 ("Even though [law enforcement] acted with restraint in conducting the search, 'the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.'") (quoting *Katz*, 389 U.S. at 356); ECF No. 48 at 15-16. The delegation of this authority to Google only demonstrates the profound lack of particularity in the geofence warrant. *See* ECF No. 48 at 16.

V. The Good Faith Exception Does Not Apply.

Mr. Chatrie fully adopts, incorporates, and re-asserts in this supplement that the *Leon* good faith exception to the exclusionary rule does not apply to evidence obtained from a warrant that was *void ab initio*. *See* ECF No. 48 at 17-20. As set forth above and in the original geofence warrant briefing, this geofence warrant is void from its inception and thus, is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh*, 540 U.S. at 558 ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law.").

Of critical importance here is the omission of key facts in the warrant affidavit that should have flagged the unique overbreadth of the search for the reviewing magistrate—namely, the true scope of the number of people to be searched and the true boundaries of the "geofence." Had the

magistrate known that the warrant he signed authorized Google to search the private daily journals of numerous tens of millions of people, surely he would have refused to sign such a warrant. Had the magistrate known that the warrant he signed simultaneously authorized a search of a church, a hotel, a restaurant, a mini storage facility, and two apartment complexes, surely he would have laid his pen on his desk and sent the affiant away empty-handed. To not include those facts demonstrates at least recklessness with regard to the true nature of the search the affiant proposed.

The unprecedented search of numerous tens of millions of private diaries at once also renders the warrant so overbroad that no reasonably objective officer would have thought it a valid warrant. *See, e.g., United States v. Winn*, 79 F. Supp. 3d 904, 923-24 (S.D. Ill. 2015) (refusing to find good faith where two officers had fifteen years of experience between them and obtained a warrant that "gave them unbridled discretion to search for and seize whatever they wished"). In *Winn*, officers used a template affidavit that received only a "quick and cursory" review by the State's Attorney to obtain "any or all files" on an individual's cell phone. *Id*. at 919, 923-24. While consultation with counsel was "prima facie evidence" of good faith, the court found that *Leon* did not apply because of the government's "recklessness" as to particularity. *Id*. at 923. The court also found that the judge "did the same . . . abandon[ing] his judicial role to some extent" by authorizing "a warrant to rummage through every conceivable bit of data." *Id*. at 923-24. Such disregard for the particularity requirement negated the government's claim of good faith in *Winn*, *id.* at 924, and it should have the same result here.

In this case the government used a warrant template (the provenance of which is still unclear to Mr. Chatrie) that was fundamentally overbroad and lacking in particularity. It substituted generalized assumptions about cell phone use for probable cause and sought to authorize the unbridled search of numerous tens of millions of Google users. It did not even attempt

to exclude devices associated with the Journey Christian Church any step along the way. The government then presented this application to a state magistrate who approved it without any information or, presumably, understanding of the scope of the search or the level of discretion being afforded to investigators. As in *Winn*, such reckless disregard for the probable cause and particularity requirements should negate the government's argument that it acted in good faith. *See also United States v. Doyle*, 650 F.3d 460, 476 (4th Cir. 2011) ("[W]here a reasonable officer would know that a probable cause determination could not be rendered without information conspicuously absent from his application for a warrant, reliance on the resulting warrant is not objectively reasonable.").

CONCLUSION

The geofence warrant here was the epitome of a general warrant, a search of numerous tens of millions of Google users in an attempt to develop a single lead. Its overbreadth and absence of particularity are so unprecedented that no officer would reasonably rely on it. As a result, this Court should suppress all evidence and fruits that the government obtained from it.

Respectfully submitted,
OKELLO T. CHATRIE

By: _____/s/_____
Michael W. Price
NY Bar No. 4771697 (*pro hac vice*)
NACDL, Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

UNITED STATES' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION FOR SUPPRESSION OF EVIDENCE OBTAINED PURSUANT TO GOOGLE GEOFENCE WARRANT

The United States of America, by its undersigned attorneys, moves this Court to deny Defendant Okello T. Chatrie's supplemental motion to suppress evidence obtained from Google, LLC ("Google") pursuant to a search warrant for GeoFence location information (the "GeoFence warrant"). ECF No. 104. This Court should deny the defendant's motion for three reasons. First, investigators did not infringe the defendant's reasonable expectation of privacy when they obtained this information from Google. Second, the GeoFence warrant complied with the Fourth Amendment, as it was issued based on probable cause and specified its object with particularity. Third, suppression is inappropriate because investigators relied on the warrant in good faith.

I. INTRODUCTION

Agents investigating the armed robbery of the Midlothian Call Federal Credit Union had good reason to believe that Google was a witness and had evidence of the crime: surveillance video showed the robber with a cell phone, and investigators knew that there was therefore a fair probability that Google had stored the robber's cell phone location information. They also knew that Google likely had other location information that would provide them with a fuller understanding of the time and place of the events of the robbery, as well as help them identify

other witnesses and suspects. Federal Bureau of Investigation Task Force Officer Josh Hylton put these facts in an affidavit, and he obtained a GeoFence search warrant for a narrowly focused set of evidence: a two-hour interval of Google location information (and associated identity information) for devices that Google's records placed within 150 meters of a point near the bank during the hour of the robbery. *See* ECF No. 54-1.

The investigators were correct: Google had been a witness to the robbery. Pursuant to the warrant, Google produced to the United States a small set of records: location information over a two-hour interval of three identified and six unidentified individuals, and limited location information over a one-hour interval of ten other unidentified individuals. This information was sufficient for investigators to recognize that the defendant's Google account likely belonged to the robber, and subsequent investigation led to his indictment.

The defendant argues that the Fourth Amendment bars Google from being a witness in an investigation like this one: that even where a judge finds probable cause to believe that Google has evidence concerning unidentified individuals present at the scene of a serious crime, the Fourth Amendment bars issuance of a warrant to obtain that evidence. Fortunately, the defendant is wrong, and his arguments that the United States violated the Fourth Amendment by obtaining his location information are without merit.

II. BACKGROUND

The United States' initial Response in Opposition to Defendant's Motion for Suppression sets forth the basic facts of the bank robbery, the GeoFence Affidavit, the GeoFence Warrant, and the warrant's execution. *See* ECF No. 41 at 1-5. In addition, Google has now submitted two affidavits relevant to the defendant's motion. *See* ECF No. 96. The United States and the defendant have agreed to stipulate to the accuracy of these affidavits. One, by Google Location

History Product Manager Marlo McGriff, describes the Google Location History service, including steps the defendant took to opt in to Google's storage of his location information. *See* ECF No. 96-1. The other, by Google Team Lead for Legal Investigations Support Sarah Rodriguez, provides further information about the execution of the GeoFence warrant. *See* ECF No. 96-2. The United States will not repeat these facts here, but will reference them below in explaining why the GeoFence warrant was consistent with the Fourth Amendment. In addition, the arguments made now by the defendant remain similar to his initial suppression arguments. The United States therefore incorporates by reference the arguments made in its initial opposition to the defendant's suppression motion and in its response to the Google amicus brief. *See* ECF No 41 at 6-24; ECF No. 71 at 1-9.

III. ARGUMENT

A. The Defendant Had No Reasonable Expectation of Privacy in Two Hours of Google Location Information

It is a fundamental Fourth Amendment principle that an individual retains no reasonable expectation of privacy in information revealed to a third party and then disclosed by the third party to the government. This principle has deep roots: when an individual discloses information to a third party, the third party becomes a witness, and it is an "ancient proposition of law" that the public "has a right to every man's evidence." *United States v. Nixon*, 418 U.S. 683, 709 (1974). The Supreme Court has repeatedly rejected Fourth Amendment arguments contrary to this principle in cases ranging from private conversations to business records. *See, e.g.*, *Hoffa v. United States*, 385 U.S. 293, 302 (1966) (statements made in the presence of an informant); *Couch v. United States*, 409 U.S. 322, 335-36 (1973) (information disclosed to an accountant); *United States v. Miller*, 425 U.S. 435, 443 (1976) (bank records); *Smith v. Maryland*, 442 U.S. 735, 742-44

(1979) (dialed telephone numbers); *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (financial records).

Based on this fundamental principle, the defendant had no reasonable expectation of privacy in the location information he disclosed to Google. As discussed below, the multiple steps that the defendant took to opt in to Google's receipt and storage of his location information confirm this result. But even without the defendant's explicit agreement to disclose his location information to Google, the defendant's voluntary disclosure of his location would be evident from the nature of the services Google provides to customers. Courts often infer that information is voluntarily disclosed to a third party based on the nature of the relationship between the third party and the one making the disclosure. For example, in *Miller*, the Supreme Court did not need to consider Miller's explicit agreements with his bank in order to conclude that he had voluntarily disclosed his financial information. Instead, the Court's conclusion was based on "examin[ing] the nature of the particular documents sought" and concluding that they were "not confidential communications but negotiable instruments to be used in commercial transactions." *Miller*, 425 U.S. at 442. Similarly, the Supreme Court's analysis of the disclosure of dialed phone numbers in *Smith v. Maryland* began by observing that telephone users "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Smith v. Maryland*, 442 U.S. at 742.

Here, similar analysis demonstrates that the defendant voluntarily disclosed his location information to Google. Google does far more than provide a storage service for its customers' location information. Instead, Google customers disclose their location to Google to obtain location-based services such as mapping, traffic updates, and help finding their phones. *See* ECF No. 96-1 at 2. For example, customers who use Google's mapping services to assist them with

driving from one place to another realize that they must convey their location to Google. Thus, because the defendant provided his location to Google to obtain its location-based services, the United States did not infringe his reasonable expectation of privacy when Google conveyed that information to the United States.

The fact that the defendant voluntarily disclosed his location information to Google is confirmed and reinforced by the multiple steps he took to enable Google to obtain and store his location. The McGriff affidavit establishes that Google users "must explicitly opt in to the [Location History] service." ECF No. 96-1 at 2. McGriff sets forth the multiple steps that a user must take before Google stores the user's Location History: Location History "functions and saves a record of the user's travels only when the user opts into [Location History] as a setting on her Google account, enables the 'Location Reporting' feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it." ECF No. 96-1 at 3.

The McGriff affidavit further explains both that Google users may delete their location information and that users are informed of this fact in the Google Privacy Policy. *See* ECF No. 96-1 at 5. Google's Privacy Policy also explains to users that Google has access to their location information for purposes ranging from providing them with targeted advertising or driving directions to Google's development of new services. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122). The defendant concedes that he "agree[d] to Google's terms and conditions during the initial setup process of his phone." ECF No. 104 at 19. As part of these terms and conditions, he agreed that Google could use his data "data in accordance with our privacy policies." *See* October 25, 2017, Google Terms of Service (available

at https://policies.google.com/terms/archive/20171025).

These facts confirm that the defendant voluntarily conveyed his location information to Google. Significantly, they also distinguish with respect to voluntary disclosure the location information here from the cell-site records of *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *Carpenter* held that cell phone users do not voluntarily disclose their cell-site records to the phone company because cell-site information is collected "without any affirmative act on the part of the user beyond powering up," because "there is no way to avoid leaving behind a trail of location data," and because carrying a cell phone "is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. These factors are not present here. Google could not obtain and store the defendant's location without his undertaking multiple affirmative acts. He had to opt in to Location History in his account settings, and he had to enable Location Reporting for his phone. *See* ECF No. 96-1 at 3. The defendant had discretion regarding whether Google stored his location information, and he retained the ability to delete it. *See* ECF No. 96-1 at 5. And none of the services associated with Google's storage of location information are indispensable to participation in modern society. The defendant thus voluntarily disclosed his location information to Google, and Google's conveyance of that information to the United States did not infringe his reasonable expectation of privacy.

The defendant makes multiple arguments in support of his claim that he had a reasonable expectation of privacy in the location information he disclosed to Google. All of them lack merit.

First, the defendant argues that *Carpenter* protects even the brief period of his location information obtained by investigators. *See* ECF No. 104 at 10-11. But this argument ignores both *Carpenter*'s explicit limitations and its reasoning. As an initial matter, the Court in *Carpenter* did not abolish the third-party doctrine or "disturb the application of *Smith* and *Miller*." *Carpenter*,

138 S. Ct. at 2220. Thus, because the defendant voluntarily disclosed his location to Google under the reasoning of *Carpenter*, the government did not conduct a search when it obtained his location information.

Even absent the third-party doctrine, *Carpenter* does not support the defendant's claim that obtaining two hours of his location information was a search. *Carpenter* protects only a privacy interest in long-term, comprehensive location information. The Court explicitly limited its holding to its conclusion "that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search." *Carpenter*, 138 U.S. at 2217 n.3. The Court emphasized that *Carpenter* was "not about 'using a phone' or a person's movement at a particular time." *Carpenter*, 138 U.S. at 2220. Instead, it was "about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* The government conducted a search in *Carpenter* because the cell-site records the government obtained created a "comprehensive record of the person's movements" that was "detailed" and "encyclopedic." *Id.* at 2216–17. By this standard, the government did not conduct a search when it obtained only two hours of the defendant's location information pursuant to the GeoFence warrant.

Significantly, although the Supreme Court decided *Carpenter* nearly two years ago, the defendant fails to cite a single case interpreting *Carpenter* broadly to protect a brief period of location information. Instead, courts have agreed that *Carpenter* protects only long-term, comprehensive location information. *See, e.g.*, *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (stating that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies))" (emphasis in original)); *Commonwealth v. McCarthy*, 484 Mass. 493, 494 (2020) ("[W]hile the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest

which potentially could be implicated by the widespread use of [automatic license plate readers], that interest is not invaded by the limited extent and use of ALPR data in this case."); *United States v. Yang*, 958 F.3d 851, 862 (9th Cir. 2020) (Bea, J., concurring) (stating that a query of a large automatic license plate recognition database that revealed only a single location point for Yang was not a search under *Carpenter* because "the information in the database did not reveal 'the whole of [Yang's] physical movements.'").[1]

Second, the defendant continues to cite the fact that the United States obtained location information regarding other Google users, *see* ECF No. 104 at 12, but he still provides no explanation of how this fact supports his claim that he had a reasonable expectation of privacy in his location information. Such an argument would be foreclosed by Supreme Court precedent. The Supreme Court has squarely held that Fourth Amendment rights "may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). Courts have agreed that defendants lack standing to challenge the government obtaining others' cell phone location information. *See, e.g.*, *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016); *United States v. Forest*, 355 F.3d 942, 948 (6th Cir. 2004), *vacated on other grounds by* 543 U.S. 1100 (2005) (vacating in light of *United States v. Booker*, 543 U.S. 220 (2005)).

[1] The defendant also cites *United States v. Karo*, 468 U.S. 705 (1984), for the proposition that the government conducts a search when it obtains "information about the interior of a constitutionally-protected space, such as a home." ECF No. 104 at 11. However, both *Smith v. Maryland* and *Hoffa* demonstrate that the government does not conduct a search when it obtains information voluntarily disclosed to another from within a protected space and then conveyed by that party to the government. *Smith v. Maryland*, 442 U.S. at 743; *Hoffa*, 385 U.S. at 301. Moreover, the defendant does not claim that the GeoFence warrant revealed any such information about him.

Third, the defendant argues that he has a reasonable expectation of privacy in the location information he disclosed to Google because Google considers it to be "'contents' for purposes of the Stored Communications Act." ECF No. 104 at 12. As the United States previously explained, Google's analysis of how the Stored Communications Act applies to location information may be incorrect. *See* ECF No. 71 at 8. But regardless, the statutory classification of Google's location information does not affect whether a user has a reasonable expectation of privacy in it. As *Hoffa* demonstrates, one has no reasonable expectation of privacy in the contents of communications disclosed to a third party when the third party conveys that information to the government. *See Hoffa*, 385 U.S. at 302. Here, because the defendant conveyed his location information to Google to obtain location-based services, his Fourth Amendment rights were not infringed when Google conveyed that information to the United States.

Fourth, the defendant argues that his Google location information should be protected because "it is at least as accurate" as the cell-site information in *Carpenter* and thus "capable of revealing the 'privacies of life.'" ECF No. 104 at 13. The United States agrees that the Google information here was at least as accurate as the cell-site information in *Carpenter*, but *Carpenter* nevertheless does not protect it both because of its short duration and because the defendant disclosed it to Google.

Fifth, despite the defendant's stipulation to the Google affidavits, he attempts to argue that he did not voluntarily disclose his location information to Google. *See* ECF No. 104 at 15-17. As an initial matter, the defendant's argument that he did not voluntarily disclose his location focuses entirely on the opt-in procedures for Google's storage of location information. He thus ignores that his voluntary disclosure of location information to Google is evident from the nature of the

location-based services (like mapping) that Google provided him.[2]

The defendant bases his argument that he did not voluntarily disclose his location information to Google in large part not on the McGriff affidavit, but instead on his own description of the setup process for an Android phone. *See* ECF No. 104 at 15-17. As an initial matter, the United States does not believe that the steps described by the defendant fully and accurately describe the steps he would have taken to create a Google account, set up the phone he used at the time of the robbery, and opt in to Google Location History. For example, the defendant does not address the steps involved in the initial creation of his Google account or signing into that account using his phone.

Nevertheless, assuming for the sake of argument that the defendant's description of his cell phone setup process is accurate, the defendant voluntarily disclosed his location information to Google. The defendant concedes that during setup, a screen on his phone informed him that "Google needs to periodically store your location to improve route recommendations, search suggestions, and more." ECF No. 104 at 15. He does not dispute that in response to this warning, he clicked "YES I'M IN." *See id.* He also concedes that this screen of his phone linked to a web page containing Google's Terms of Service and Privacy Policy, *see id.* At 15-16, which describe

[2] Although the defendant might object that a user of Google's location-based services cannot tell that Google will store her location information, the Supreme Court held in *Smith v. Maryland* that the third-party doctrine applies to information voluntarily disclosed to a third party regardless of any expectations regarding subsequent storage. In *Smith*, the defendant argued that the third-party doctrine should not apply to his dialed numbers because the phone company did not usually store information concerning local phone calls. The Supreme Court rejected his argument: "The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record." *Smith*, 442 U.S. at 745. Thus, the defendant would have no reasonable expectation of privacy in information he disclosed to Google even if he had not been informed that Google would store that information.

Google's use, storage, and deletion of location information. He further concedes that he "would have had to agree" to these terms and conditions. ECF No. 104 at 19.

These concessions are fatal to the defendant's argument that he did not voluntarily disclose his location information to Google. The defendant attempts to evade the consequences of his agreements through an argument worthy of Goldilocks: that the language on his phone screen was too short, and that the Terms of Service and Privacy Policy were too long. He complains that the language on his phone screen did not use the phrase "Location History" or inform him "of the privacy implications of turning it on," and he complains that the Privacy Policy was "27 pages long." *See* ECF No. 104 at 15-16. But the language on his phone screen was just right—in brief, clear language, it informed him of what Google would do: periodically store his location to provide him with services. Moreover, the Supreme Court has never limited voluntary disclosure under the third-party doctrine to circumstances where one is informed of the Fourth Amendment implications of disclosure. And the Privacy Policy was also just right, because it gave the defendant the opportunity to obtain a more detailed explanation of Google's use and storage of his location information.

Sixth and finally, the defendant cites cases addressing whether Internet Terms of Service create binding contacts, including a case within this district enforcing such a contract. *See* ECF No. 104 at 18-20 (citing *Melo v. Zumper*, No. 3:19-cv-621 (DJN), 2020 WL 465033 (E.D. Va. Jan. 28, 2020)). Although Google's Terms of Service likely creates a binding contract with customers, the defendant cites no cases holding that this contracts question plays any role in determining whether information is voluntarily disclosed to a third party for Fourth Amendment purposes. For example, the Supreme Court in *Smith v. Maryland* relied on statements in phone books to support its conclusion that "telephone users realize that they must 'convey' phone numbers to the telephone

company," *Smith v. Maryland*, 442 U.S. at 742-43, but phone book statements are not likely part of a contract between a phone company and its customers.

Moreover, courts rely on terms of service in evaluating whether a service provider's disclosure of information to the government violates the Fourth Amendment. *See, e.g.*, *Adkinson*, 916 F.3d at 610 (holding that that T-Mobile's disclosure of cell-site information to the government did not violate Adkinson's Fourth Amendment rights because Adkinson "agreed to T-Mobile's policy that T-Mobile could disclose information when reasonably necessary to protect its rights, interests, property, or safety"). Here, the defendant agreed that in order to obtain Google's location-based services, he would share his location with Google, and he chose for Google to store it. Google's conveyance of that information to investigators did not infringe his reasonable expectation of privacy.[3]

B. The Fourth Amendment's Protection of Property Does Not Restrict Google from Conveying to the United States Information Disclosed to it by the Defendant

The defendant continues to argue that obtaining location records from Google was a search under "a property based theory," *See* ECF No. 104 at 20, but his argument flies in the face of the fundamental principle that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443. The Supreme Court has recognized that a physical trespass for purposes of obtaining

[3] The defendant also cites European complaints regarding Google's storage of location information. For example, the defendant cites a complaint by a Norwegian individual whose name is redacted in which that unknown person alleges that Google "uses different means to nudge the user into turning on" Location History. *See* ECF No. 104 at 17 (citing complaint available at https://fil.forbrukerradet.no/wp-content/uploads/2018/11/complaint-google-27-november-2018-final.pdf). Here, where this Court has the benefit of an expert from Google, as well as experts provided by the United States and the defense, this Court should not rely on unproven allegations from an anonymous person abroad.

information is a search. *See United States v. Jones*, 565 U.S. 400, 404-05 (2012). But the investigation in this case involved no physical trespass; instead, the GeoFence warrant directed Google to produce specified information that its customers had disclosed to it. The defendant cites no case—and the United States is aware of no case—in which a court has relied on a "property-based theory" to discard the third-party doctrine of *Smith* and *Miller* or prevent witnesses from providing evidence to the government. Justice Gorsuch's solo dissent in *Carpenter* did contemplate abandoning the third-party doctrine based on some sort of property rights theory of the Fourth Amendment, *see Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J., dissenting), but a solo dissent is not the law, and the third-party doctrine of *Smith* and *Miller* remains binding law.

In addition, the defendant's assertion that Google is a "mere bailee" of location information ignores how Google uses location information to provide services to its customers. ECF No. 104 at 20. Google does not merely store its customers' locations; it uses that information to provide location-based services. *See* ECF No. 96-1 at 2. Under these circumstances, Google's disclosure of its customers' location information to investigators does not implicate the Fourth Amendment. For example, the owner of documents may retain a property interest in documents shared with an accountant, but the owner's Fourth Amendment rights are not infringed when the accountant conveys them to the government. *See Couch*, 409 U.S. at 335.

C. The GeoFence Search Warrant Satisfied the Fourth Amendment

The GeoFence warrant satisfied the Fourth Amendment because it was issued on a showing of probable cause and specified its object with particularity. The defendant's arguments that the search warrant did not "meet the probable cause or particularity requirements demanded by the Fourth Amendment" are without merit. ECF No. 104 at 22.

1. The Geofence Affidavit Established Probable Cause

Probable cause requires only "a fair probability, and not a prima facie showing, that contraband or evidence of a crime will be found in a particular place." *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (internal quotation marks omitted)). Here, the affidavit in support of the Geofence warrant established an ample basis for the issuing magistrate's finding of probable cause. In particular, the affidavit established: (1) that an unknown subject committed an armed bank robbery at a particular place and time; (2) that prior to the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone; (3) that the majority of cell phones were smartphones; (4) that "[n]early every" Android phone "has an associated Google account," and that Google "collects and retains location data" from such devices when the account owner enables Google location services; and (5) that Google can collect location information from non-Android smartphones if the devices are "registered to a Google account and the user has location services enabled." State GeoFence Warrant at 4-5. From this information, there was a substantial basis for the magistrate to find probable cause to believe that Google possessed evidence related to the robbery.

The defendant argues that the warrant lacked probable cause because it "did not identify any individuals or accounts to be searched because investigators did not know who they were searching for, or even if Google would have relevant data." ECF No. 104 at 22. However, a warrant for evidence of crime need not identify specific individuals or establish with certainty that evidence will be found—all it must do is establish a fair probability that specified evidence will be found in the place to be searched. Indeed, the warrant here is similar in this respect to the search warrant approved by the Supreme Court in *Zurcher v. Stanford Daily*, 436 U.S. 547, 551 (1978), which authorized seizure from a newspaper of photographs of unidentified individuals who had

assaulted police officers.

The defendant also ignores the standard for probable cause when he argues that probable cause was lacking because "the application rested on broad conjecture based on the popularity of Google and cell phones generally." ECF No. 104 at 22. As an initial matter, the affidavit included specific facts supporting the finding of probable cause, including the robbery itself and that the armed robber had a cell phone. Moreover, it is entirely appropriate in the Fourth Amendment context to rely in part on probabilistic inferences. For example, *in United States v. James*, No. 18-cr-216, 2019 WL 325231, at *3 (D. Minn. Jan. 25, 2019), the court relied on inferences about cell phone use to conclude that a warrant for a cell tower dump was based on probable cause, even though it was "unknown whether a phone was used by the suspect before or after the robbery."[4] As required by the Fourth Amendment, the GeoFence affidavit established a fair probability that Google had evidence pertaining to the robbery.

2. The GeoFence Warrant Was Not Overbroad

Under the Fourth Amendment, "a valid warrant must particularly describe the place to be searched, and the persons or things to be seized." *United States v. Kimble*, 855 F.3d 604, 610 (4th Cir. 2017) (internal quotation marks omitted). The Fourth Amendment constrains a warrant so that it is "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). It protects against "exploratory rummaging in a person's belongings." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (quoting *Andresen v.*

[4] The recent Supreme Court case *Kansas v. Glover*, 140 S. Ct. 1183 (2020), provides an example of the Court upholding probabilistic reasoning in the Fourth Amendment context. The Court held that a police officer had properly made a "commonsense inference" that the owner of a vehicle was likely its driver. *Id.* at 1188. *See also Illinois v. Gates*, 462 U.S at 240 (noting the authority of a magistrate issuing a search warrant "to draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant").

Maryland, 427 U.S. 463, 480 (1976)). Moreover, the test "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d 743, 745 (8th Cir. 1976)).

Here, the GeoFence warrant was limited based on location, dates, and times. The warrant sought only location and identity information from Google regarding a two-hour interval for individuals present at the site of an armed robbery during a one-hour interval. The warrant was appropriate for its investigatory purpose, which was to obtain evidence to help identify and convict the robber. The warrant's breadth is also supported by *James*, in which the district court held that a cell tower dump warrant was sufficiently limited because it was constrained geographically and temporally to robberies under investigation. *James*, 2019 WL 325231 at *3. The GeoFence warrant here is narrower than the warrant upheld in *James*: its geographical area was smaller than a cell site, and it produced information about only 19 individuals, as opposed to "hundreds if not thousands." *Id.*

The defendant argues that the GeoFence warrant was overbroad because Google reviewed a large body of data in order to comply with it, *see* ECF No. 104 at 22-24, but this argument is without merit. He cites no case law holding that a service provider may not review a large data set in order to produce a narrowly defined set of information. Such process is not new: for example, phone companies may review every call made by all their customers in order to find calls made to a specified phone number. *See Ameritech Corp. v. McCann*, 403 F.3d 908, 910 (7th Cir. 2005). GeoFence warrants are also similar to tower dump warrants: they determine who was present at a particular place and a particular time. If the cell tower is in a busy area, a large set of customers may have used the tower; the phone company in response to the warrant must search

within that data for those who used the tower at the specified time.

Google's review of a large set of data to comply with the GeoFence warrant is a result of Google's internal data storage practices, not an overbroad warrant. It would be possible for Google to create an additional Location History database indexed by location. This database would enable Google to comply with a GeoFence warrant—and produce the exact same data as Google currently produces—without reviewing the data of all customers. The constitutionality of a search warrant does not depend on a service provider's internal data storage practices which are invisible to customers and the government alike. Thus, the appropriate measure for the breadth of the GeoFence warrant is the limited data sought by the warrant, which resulted in the government obtaining location information for only 19 individuals, all of whom were near the bank at the time of the robbery.

3. The GeoFence Warrant Was Sufficiently Particular

The defendant next argues that the GeoFence warrant was insufficiently particular because of its three-step process, but the defendant's arguments are mistaken. First, the defendant complains that "Google decided to search only a portion of its records, specifically 'Location History' records." *See* ECF No. 104 at 25. As an initial matter, even if Google should have reviewed additional databases for responsive information, Google's failure to do so would not demonstrate any infirmity in the warrant or infringe the defendant's Fourth Amendment interests. No Stored Communications Act warrant has even been written that a service provider cannot botch, but a service provider's failure to produce a portion of the information sought pursuant to a warrant does not violate the Fourth Amendment. But as Google explains, it did nothing wrong: Location History was "the only form of location data Google maintains that Google believes to be responsive to a geofence request." McGriff Affidavit at 7. Google's review and production of the

information that it believed fell within the scope of the warrant does not make the warrant insufficiently particular. There was no reason for Google to review information it had concluded was nonresponsive to the warrant. [5]

Second, the defendant complains that Google's response to the warrant was not dependent on Google's estimates of the margins of error associated with its location calculations. *See* ECF No. 104 at 25. It is certainly true that no cell phone location measurement has perfect accuracy. However, a warrant that does not adopt a probabilistic approach to all location information is not insufficiently particular. Here, the warrant directed Google to disclose information for devices "inside the described geographical area" during the time of the robbery, and Google correctly interpreted this to mean it should disclose information concerning devices that its calculations placed within the circle specified by the warrant. Although there always remains a possibility of inaccuracy in Google's location information, and a defendant may certainly challenge at trial the weight given to this information, the possibility of inaccuracy does not make a warrant insufficiently particular.[6]

Third, the defendant argues that the warrant was insufficiently particular based on the correspondence between Google and FBI TFO Josh Hylton regarding step 2 of the warrant, but

[5] Elsewhere in his motion, the defendant states that the 'warrant required Google to produce location data for 'each type' of Google account," and he faults Google for not producing data from the Web & App Activity or Google Location Accuracy databases. ECF No. 104 at 7. The defendant has misinterpreted the GeoFence warrant: Web & App Activity and Google Location Accuracy are separate Google services, not separate types of Google accounts.

[6] The defendant does not dispute that his Google location information would have fallen within the scope of the warrant regardless of how the warrant addressed the uncertainty associated with it. Instead, the defendant highlights a single Google measurement of someone else's phone with a margin of error of 387 meters. *See* ECF No. 104 at 25. Another measurement associated with that person's device, however, had a margin of error of only 84 meters, placing the device within the GeoFence region.

this correspondence provides no evidence that the warrant lacked particularity. *See* ECF No. 104 at 25-26. The warrant was sufficiently particular because it specified the evidence law enforcement was authorized to obtain: two hours of location data (and associated identity information) for all individuals present at the site of the robbery during the hour of the robbery. The step 2 correspondence addresses an entirely separate issue: FBI TFO Hylton's decision to obtain less than the maximum amount of information authorized by the warrant. The Fourth Amendment requires that the information specified by a warrant must be "no broader than the probable cause on which it is based," *Hurwitz*, 459 F.3d at 473, but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. Indeed, a contrary rule would be perverse: agents executing warrants would be required to engage in more invasive searches than they deemed necessary, simply because they had previously established probable cause for additional evidence.

Agents executing warrants often make choices about the intensity of their execution of a search warrant, and it is not a Fourth Amendment violation if they ultimately leave some evidence behind. The Playpen warrant explicitly included such a provision: it authorized a search of the computer of everyone who visited a specified child pornography web site, but it also stated that "in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users." *United States v. Anzalone*, 208 F. Supp. 3d 358, 363 (D. Mass. 2016). Courts uniformly agreed that this provision did not violate the Fourth Amendment's particularity requirement. *See, e.g.*, *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016) ("[T]he fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site"). The defendant attempts to distinguish the Playpen warrant based on its breadth, *see* ECF No. 104 at 23-24, but the United

States cites the Playpen warrant for an entirely different proposition: that it is permissible for a warrant to authorize investigators to seize less than the maximum amount of evidence for which they have established probable cause and which the warrant describes with particularity. FBI TFO Hylton did not violate the Fourth Amendment when he executed the warrant in a manner that provided additional privacy protections for the majority of individuals present at the robbery. [7]

Nor was there anything improper about FBI TFO Hylton's correspondence with Google, in which he ultimately requested that Google produce step 2 location information about nine individuals. Google remains an independent actor, and courts have held that a provider like Google has a due process right to object to an order directing it to comply with a search warrant. *See, e.g.*, *In re Application*, 610 F.2d 1148, 1157 (3d Cir. 1979). Where a service provider produces a portion of the information specified by legal process, the United States does not violate the Fourth Amendment when it chooses not to litigate over the rest. A contrary rule would waste judicial resources and harm privacy. Nothing in the execution of the GeoFence warrant supports the defendant's argument that the warrant was insufficiently particular.

Finally, arguing that "every person takes a 'unique path through life,'" the defendant also faults the warrant for stating that the information produced by Google in step 1 and step 2 would be "anonymized." ECF No. 104 at 27. In the context of the GeoFence warrant, however, "anonymized information" refers to the fact that Google did not produce its subscriber identity information associated with the location information until step 3 of the warrant. The GeoFence warrant's use of the phrase "anonymized information" does nothing to make the warrant insufficiently particular.

[7] As argued in its initial opposition to the defendant's suppression motion, if the three-step process for the GeoFence warrant were insufficiently particular, the proper remedy would be to sever the second step. *See* ECF No. 41 at 20-21.

D. Evidence from the GeoFence Warrant Should Not Be Suppressed Because Investigators Relied upon it in Good Faith

Even assuming the GeoFence warrant was lacking in probable cause or particularity, suppression would not be an appropriate remedy. In its response to the defendant's initial suppression motion, the United States explained that the good faith exception precluded suppression in this case both under the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984), and under the Fourth Circuit's standard in *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), for good-faith reliance on a search warrant authorizing use of a novel investigative technique. *See* ECF No. 41 at 21-24. The United States will not repeat these arguments here, but they remain fully applicable to the defendant's supplemental motion.

The defendant now advances an additional argument against the good faith exception: he claims that the good-faith exception should not apply here because the GeoFence affidavit omitted "the true scope of the number of people to be searched and the true boundaries of the 'geofence.'" ECF No. 104 at 28. To challenge a search warrant on this basis, the defendant would be required to show "(1) that the officer deliberately or recklessly omitted the information at issue and (2) that the inclusion of this information would have defeated probable cause." *United States v. Andrews*, 577 F.3d 231, 238-39 (4th Cir. 2009). Here, the defendant's argument fails because he cannot satisfy either of these requirements.

To begin, the information that the defendant asserts should have been included in the warrant would not have defeated probable cause. First, information about Google's internal data structures and how it processes GeoFence warrants has nothing to do with either the probable cause that supported the warrant or the information that the warrant authorized to be seized. Instead, it relates to how the warrant was executed, and the Supreme Court has held that "[n]othing in the

language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the three requirements discussed above [a neutral magistrate, probable cause, and particularity], search warrants also must include a specification of the precise manner in which they are to be executed." *Dalia v. United States*, 441 U.S. 238, 257 (1979). Regardless of how Google organized its databases or executed the warrant, the affidavit established a fair probability that Google had evidence of the location of the armed robber and others at the time of the robbery. Similarly, the fact that there is some margin of error in all service provider cell phone location information does not undermine probable cause or particularity: the affidavit still would have established a fair probability that Google stored location information of the robber and other nearby witnesses.[8]

Nor can the defendant establish that any omission by FBI TFO Hylton was deliberate or reckless. There was no reason for TFO Hylton even to know about the organization of Google's internal data structures. The defendant therefore cannot show that any omission regarding that information was deliberate or reckless. And the fact that there is some error in cell phone location measurements is common knowledge; there is no reason Officer Hylton would not have expected the issuing judge to be aware of that fact. In sum, the omissions cited by the defendant were not material to the issuance of the warrant, and in any event the defendant has not shown that any omissions were deliberate or reckless.

Finally, the defendant's argument against the good-faith exception relies heavily on a

[8] For example, the affidavit could have included the fact that many of Google's location points are based on GPS information, and that GPS coordinates are usually accurate to within a few feet. *See* https://www.gps.gov/systems/gps/performance/accuracy. This additional information would not have defeated the affidavit's probable cause. FBI TFO Hylton could not have known in advance Google's confidence radii for its WiFi-based location points. But even if he could have known that the step 1 WiFi location points would end up having a median confidence radius of 25 meters, that fact also would not have affected the existent of probable cause.

district court case from another circuit, *United States v. Winn*, 79 F. Supp. 3d 904 (S.D. Ill. 2015). But the warrant in *Winn* was nothing like the warrant here: it authorized seizure of "any or all files" contained on a cell phone. *Winn*, 79 F. Supp. 3d at 918. Here, in contrast, the warrant was remarkably targeted: despite the vast quantity of data stored by Google, it targeted only two hours of location data associated with devices near the bank at the time of the armed robbery, and Google produced data regarding only 19 accounts. Officers' reliance on the warrant was reasonable, and this Court should deny the defendant's motion to suppress.

IV. CONCLUSION

For the reasons set forth in this brief, this Court should deny the defendant's motion to suppress the fruits of the GeoFence warrant.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 12th day of June, 2020, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koenig
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorney
Office of the United States Attorney
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Richmond Division (The Hon. M. Hannah Lauck)

JOINT APPENDIX

VOLUME 3 of 11 (pages 417 - 694)

JESSICA D. ABER
United States Attorney

Kenneth R. Simon, Jr., Ass't U.S. Attorney
Peter S. Duffey, Ass't U.S. Attorney
Counsel for Appellee
919 East Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400

Nathan P. Judish, Senior Counsel
Computer Crime & Intel. Property Section
Criminal Division
U.S. Department of Justice

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
Counsel for Appellant
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800

Michael W. Price, Litigation Dir.
NACDL Fourth Amendment Ctr.
1660 L Street NW, 12th Floor
Washington, DC 20036

This page intentionally left blank for double-sided pagination and printing

TABLE OF CONTENTS

VOLUME 1 (pages 1 - 176)

District Court Docket Sheet (as of Jan. 17, 2023) 1

Indictment (Sept. 17, 2019, Doc. 1) 22

Defendant's Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Oct. 29, 2019, Doc. 29) 25

Government's Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (Nov. 19, 2019, Doc. 41) 51

Defendant's Reply to Government's Response [to] Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Dec. 9, 2019, Doc. 48) 76

Exh. A (First Step 2 Request to Google) (Doc. 48-1) 98
Exh. B (Second Step 2 Request to Google) (Doc. 48-2) 100
Exh. C (Third Step 2 Request to Google) (Doc. 48-3) 102
Exh. D (Transcript, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019)) (Doc. 48-4) ..... omitted from J.A.

Government's Notice Regarding Attachment of Google Geofence State Search Warrant to Response in Opposition to Motion to Suppress (Dec. 18, 2019, Doc. 54) 104

Affidavit for search warrant and warrant, with attachments (Doc. 54-1) 107

Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant (Dec. 20, 2019, Doc. 59-1) 118

United States' Response to Amicus Curiae Brief of Google LLC (Jan. 10, 2020, Doc. 71) 148

Defendant's Response to Google's Motion to File Amicus Curiae Brief in Support of Neither Party (Jan. 10, 2020, Doc. 72) 158

VOLUME 2 (pages 177 - 416)

Transcript, Discovery Motion Hearing (Jan. 21, 2020, Doc. 81; *see* Doc. 77 (court minutes))....177

Preliminary matters....179

Def't witness Spencer McInvaille — Direct examination....193; Cross examination....283; Redirect examination....306

Argument by the defense....318
Argument by the government....332
Rebuttal by the defense....350

Court's ruling....355

Defendant's Supplemental Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (May 22, 2020, Doc. 104)....363

United States' Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (June 12, 2020, Doc. 109)....393

VOLUME 3 (pages 417 - 694)

Transcript, Suppression Motion Hearing, Day 1 (evidence) (Mar. 4, 2021, Doc. 201; *see* Doc. 198 (court minutes))....417

Preliminary matters....420

Def't witness Spencer McInvaille — Direct examination....432; Cross examination....542; Redirect examination....586

Def't witness Marlo McGriff — Direct examination....606

VOLUME 4 (pages 695 - 1070)

Transcript, Suppression Motion Hearing, Day 2 (evidence) (Mar. 5, 2021, Doc. 202; *see* Doc. 199 (court minutes)) 695

Preliminary matters 698

Def't witness Marlo McGriff, cont'd — Direct examination ..... 699; Cross examination ..... 791; Redirect examination 841

Def't witness Sarah Rodriguez — Direct examination ..... 862; Cross examination ..... 902; Redirect examination 916

Gov't witness Jeremy D'Errico — Direct examination ..... 923; Cross examination ..... 967; Redirect examination 1010

Gov't witness Joshua Hylton — Direct examination ..... 1016; Cross examination ..... 1040; Redirect examination 1063

Concluding matters 1064

VOLUME 5 (pages 1071 - 1326)

Defendant's Post-Hearing Brief on "Geofence" General Warrant (May 3, 2021, Doc. 205) 1071

Government's Response in Opposition to Defendant's Motion for Suppression (May 21, 2020, Doc. 214; *see* Doc. 207-2) 1117

Defendant's Reply to Government's Response in Opposition to Motion for Suppression (June 4, 2020, Doc. 213) 1164

Transcript, Suppression Hearing (arguments) (June 24, 2021, Doc. 217; *see* Doc. 215 (court minutes)) 1185

Argument by the defense 1187
Argument by the government 1231
Rebuttal by the defense 1313

Concluding matters 1322

VOLUME 6 (pages 1327 - 1456)

Memorandum Opinion (denying suppression motion) (Mar. 3, 2022, Doc. 220) 1327

Order (denying suppression motion) (Mar. 3, 2022, Doc. 221) 1390

Criminal Information (May 6, 2022, Doc. 224) 1391

Transcript, Change of Plea Hearing (May 9, 2022, Doc. 247; *see* Doc. 226) 1394

Plea Agreement (May 9, 2022, Doc. 228) 1428

Statement of Facts (May 9, 2022, Doc. 229) 1444

Judgment in a Criminal Case (Aug. 19, 2022, Doc. 239) 1449

Notice of Appeal (Aug. 25, 2022, Doc. 241) 1456

VOLUME 7 (pages 1457 - 1810) – DOCUMENT EXHIBITS

Exhibits Admitted at Discovery Motion Hearing (Jan. 21, 2020)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) ..... *see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) ..... *see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) ..... *see* J.A. 2093
Def't Exh. 4: Activation Video ..... omitted from J.A., available on request
Def't Exh. 5: Three Paths Video (sealed) ..... *see* J.A. 2139
Def't Exh. 6: First Step 2 Request to Google 1457
Def't Exh. 7: Second Step 2 Request to Google 1459
Def't Exh. 8: Third Step 2 Request to Google 1461

Def't Exh. 9: Step 3 Request to Google 1463

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) .....*see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) .....*see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) .....*see* J.A. 2093
Def't Exh. 5: Three Paths Video (sealed) .....*see* J.A. 2139
Def't Exh. 6: Spencer McInvaille Report 1464
Def't Exh. 7: Spencer McInvaille Supplemental Report 1469
Def't Exh. 8: CSV Google Data File (.csv file) .....*see* J.A. 2139
Def't Exh. 9: Unique in Crowd Study 1475
Def't Exh. 11: September 2018 Oracle Submission 1480
Def't Exh. 18: Federal Search Warrant Application & Attachments 1502
Def't Exh. 19: State Search Warrants & Attachments 1534
Def't Exh. 21: McGriff Declaration 1 (Doc. 96-1) 1551
Def't Exh. 23: McGriff Declaration 3 (Doc. 147) 1562
Def't Exh. 24: Rodriguez Declaration (Doc. 96-2) 1579
Def't Exh. 27: Every Step You Take 1587
Def't Exh. 30: AZ Ex. 18 (admitted portions only) 1631
Def't Exh. 31: AZ Ex. 19 (admitted portions only) 1633
Def't Exh. 32: AZ Ex. 20 1639
Def't Exh. 33: AZ Ex. 24 1644
Def't Exh. 34: AZ Ex. 202 1667
Def't Exh. 36: AZ Ex. 209 1777
Def't Exh. 38: AZ Ex. 219 1781
Def't Exh. 40: AZ Ex. 236 1797
Def't Exh. 41: AZ Ex. 260 1804

VOLUME 8 (pages 1811 - 2090) – DOCUMENT EXHIBITS, CONT'D

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021), cont'd

Def't Exh. 43: May 2018 Privacy Policy – Redline 1811
Def't Exh. 43a: May 2018 Privacy Policy – Redline (with internet source information) 1840
Def't Exh. 44: Jan. 2019 Privacy Policy – Redline 1865
Def't Exh. 45: Oct. 2019 Privacy Policy – Redline 1895
Def't Exh. 46: McGriff Blog 1 1926

Def't Exh. 47: McGriff Blog 2 1929
Def't Exh. 48: 2018 Quartz Article 1934
Def't Exh. 49: 2018 AP Article 1 1941
Def't Exh. 51: 2019 NYT Article 1948
Def't Exh. 53: Blumenthal-Markey Letter to FTC 1957

Gov't Exh. 1: CAST PowerPoint Presentation 1981
Gov't Exh. 2: Geofence Warrant (Doc. 54-1) ..... *see* J.A. 107
Gov't Exh. 3: Declaration of Marlo McGriff (Mar. 11, 2020)
(same as Def't Exh. 21 (Doc. 96-1)) ..... *see* J.A. 1551
Gov't Exh. 3a: Declaration of Sarah Rodriguez (Mar. 11, 2020)
(same as Def't Exh. 24 (Doc. 96-2)) ..... *see* J.A. 1579
Gov't Exh. 3b: Supplemental Declaration of McGriff (June 17, 2020)
(Doc. 110-1) 2032
Gov't Exh. 3c: Third Declaration of Marlo McGriff (Aug. 7, 2020)
(same as Def't Exh. 23 (Doc. 147)) ..... *see* J.A. 1562
Gov't Exh. 4: Joshua Hylton emails with Google 2034
Gov't Exh. 5: Google Privacy Policy 2048
Gov't Exh. 5a: Google Terms of Service 2081
Gov't Exh. 6: Special Agent D'Errico's C.V. 2088
Gov't Exh. 12: "Got to Be Mobile" Video ..... *see* J.A. 2091

VOLUME 9 (pages 2091 - 2092) – DIGITAL MEDIA EXHIBIT

Gov't Exh. 12: "Got to Be Mobile" Video (admitted only at suppression motion hearing) ..... (.mp4 file)

VOLUME 10 (pages 2093 - 2138) – SEALED DOCUMENT EXHIBIT

Def't Exh. 3: PDF of Raw Data (*see* Doc. 69 (sealing order)) (admitted at both discovery motion hearing and suppression motion hearing) 2093

VOLUME 11 (pages 2139 - end) – SEALED DIGITAL MEDIA EXHIBITS

Def't Exh. 5: Three Paths Video (admitted at both discovery motion hearing and suppression motion hearing) ..... (.mp4 file)
Def't Exh. 8: CSV Google Data File (admitted only at suppression motion hearing) ..... (.csv file, viewable in Excel)

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA	
v.	Criminal No. 3:19CR130
OKELLO T. CHATRIE	March 4, 2021

DAY ONE

COMPLETE TRANSCRIPT OF MOTION TO SUPPRESS
BEFORE THE HONORABLE M. HANNAH LAUCK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

Kenneth R. Simon, Jr., Assistant U.S. Attorney
Peter S. Duffey, Assistant U.S. Attorney
U.S. Attorney's Office
SunTrust Building
919 East Main Street, Suite 1900
Richmond, Virginia 23219

Nathan P. Judish, Assistant U.S. Attorney
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, Virginia 20530

Counsel for the United States

Laura J. Koenig, Assistant Federal Public Defender
Paul G. Gill, Assistant Federal Public Defender
Office of the Federal Public Defender
701 E. Broad Street, Suite 3600
Richmond, Virginia 23219

Counsel for the Defendant

DIANE J. DAFFRON, RPR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT

APPEARANCES: (Cont'd)

Michael W. Price, Esquire
National Association of Criminal Defense Lawyers
1660 L Street, NW
12th Floor
Washington, DC 20036

Counsel for the Defendant

I N D E X

	DIRECT	CROSS	REDIRECT
SPENCER McINVAILLE	16	126	170
MARLO McGRIFF	190	--	--

E X H I B I T S

DEFENDANT'S EXHIBITS:		Page
No. 1	Geofence Warrant and Application	27
No. 2	Google Amicus Curiae Brief	200
No. 3	PDF of Raw Data	34
No. 5	Three Paths Video	61
No. 6	Spencer McInvaille Report	75
No. 7	McInvaille Supplemental Report	81
No. 8	CSV Google Data File	120
No. 11	September 2018 Oracle Submission	92
No. 21	McGriff Declaration 1	52
No. 23	McGriff Declaration 3	73

E X H I B I T S

		Page
DEFENDANT'S EXHIBITS: (Cont'd)		
No. 27	Every Step You Take	96
No. 30	AZ Ex. 18	255
No. 31	AZ Ex. 19	258
No. 32	AZ Ex. 20	249
No. 33	AZ Ex. 24	250
No. 34	AZ Ex. 202	252
No. 36	AZ Ex. 209	243
No. 38	AZ Ex. 219	227
No. 40	AZ Ex. 236	245
No. 43	2018 Privacy Policy - Redline	261
No. 46	McGriff Blog 1	219
No. 47	McGriff Blog 2	218
No. 48	2018 Quartz Article	85
No. 49	2018 AP Article 1	225
No. 53	Blumenthal-Markey Letter to FTC	233
GOVERNMENT'S EXHIBITS:		
No. 1	CAST Report	32

(The proceedings in this matter commenced at 9:30 a.m.)

THE CLERK: Case No. 3:19CR130, United States of America versus Okello Chatrie.

The United States is represented by Kenneth Simon, Peter Duffey, and Nathan Judish.

The defendant is represented by Paul Gill, Laura Koenig, and Michael Price.

Are counsel ready to proceed?

MR. SIMON: The United States is ready, Your Honor.

MS. KOENIG: The defense is ready, Your Honor.

THE COURT: Okay.

MS. KOENIG: Before we begin --

THE COURT: Okay. I'm aware that we have counsel for Google here. I don't know if you want to just state your name on the record because that you will be representing witnesses that come forward. It's really up to you.

MS. CARROLL: Thank you, Your Honor. Catherine Carroll, present on behalf of Google.

THE COURT: Thank you.

MR. CARROLL: Thank you.

THE COURT: All right. Well, I understand that you all have handled some logistics, that the defense will begin presenting evidence first. I'll hear any introductory remarks that either side wants to present. And I think there's something else you wanted to address, and I can't remember.

MS. KOENIG: Yes, Your Honor. We have a modified sequestration order that the parties have agreed to that we're asking the Court to enter. Shall I just come to the podium?

THE COURT: Yes.

MS. KOENIG: Each party has an advisory witness. The defense will designate Spencer McInvaille, who's our expert, as our advisory witness, and ask that he be allowed to remain in the courtroom throughout the proceedings.

The government, I understand, will be designating Detective Hylton, who is their case agent as their advisory witness. The government also has an additional expert, Agent D'Errico, and so he will also be allowed to remain in the courtroom in an expert capacity. But we are asking that the witnesses, in order that the witnesses -- any other witnesses not be allowed to be in the courtroom, except for during their testimony.

THE COURT: All right.

MS. KOENIG: And then the last piece of it is that the witnesses are not allowed to discuss their testimony with other witnesses.

THE COURT: Right. And, obviously, counsel aren't allowed to talk about testimony that's coming in.

MS. KOENIG: So that is -- that's the modification, Your Honor, is that the parties have agreed that counsel will be able to talk to witnesses, but the witnesses will not be able to talk to each other.

THE COURT: So that includes Google?

MS. KOENIG: Correct.

THE COURT: All right. Now, I'm going to ask you to spell the names on the record because I know Hylton is spelled differently than a court reporter might think, and just to be sure that we get everything correct.

MS. KOENIG: Sure. The defense expert is Spencer McInvaille. M-c-I-N-V-A-I-L-L-E. And Detective Hylton is H-Y-L-T-O-N. And Agent D'Errico, I don't believe there's an apostrophe. Oh, there is. Okay. D-apostrophe-E-R-R-I-C-O. The spelling of the agent was not my preparation today. Thank you.

THE COURT: Does the government have anything to add?

MR. SIMON: Nothing from us, Judge.

THE COURT: All right. So we will enter the modified sequestration order. Obviously, counsel will be responsible in making sure that their witnesses know not to speak to each other. My bet is they already know that, given the counsel that we have in front of us. And we'll certainly allow the experts to hear the evidence as it goes in. That's not uncommon and will, I think, serve the interests of the hearing overall.

Do we have folks calling in or not?

THE CLERK: Yes, ma'am. I have the line set up, but it doesn't appear that anybody is on there at this time.

THE COURT: Okay. So I want you to know we've had some folks ask to call in on an AT&T line. Of course, it's as if we're in open court. I've okayed that. If you are aware of anybody who you know who is calling in, I'm going to require counsel to inform them of our Local Rule 53 and the standing order that they cannot record or transmit or give any kind of broadcast of this hearing. We are in the hearing. Ms. Daffron will create our record. And

especially with an AT&T line, it's a little odd, and we're only really doing this because of COVID. I just want to be sure that they are aware that even if they sort of want to save something to tell a friend, or somebody who might have an interest in the case, they just cannot. They can order a transcript, but they can't do anything more than that.

MS. KOENIG: Your Honor, I will tell the Court that we expect that several members of the NACDL staff --

THE COURT: So you have to talk slower and say N-A-D-C-L more clearly.

MS. KOENIG: Thank you. I expect that several members, staff members, of NACDL, which is the organization that Mr. Price works for, will be calling in. We are a little surprised they haven't called in already. But they have already been instructed not to do any recordings or --

THE COURT: We'll say it to anybody who does call in.

THE CLERK: Hopefully, he can hear us.

THE COURT: Can we confirm that he can?

THE CLERK: Mr. Shoop, can you hear us? No.

THE COURT: So we have somebody from NBC calling in?

THE CLERK: Yes.

THE COURT: I want to be sure that that person knows. I have to announce that so he or she can hear it, too.

THE CLERK: It is NBC Universal.

THE COURT: Okay. NBC Universal. My apologies for the delay.

MR. PRICE: Your Honor, we just got word that lots of people are on the line considering the beeps, but no one can hear anything.

THE COURT: They can't hear.

THE CLERK: All right. I'm going to have to call Martin.

THE COURT: All right. So we have to get our IT involved. While we're waiting, what I'd like to be sure is that we put on the record the motion we're taking evidence for and other sort of just standard things.

MS. KOENIG: Yes, Your Honor. I don't expect that the defense will have any introductory remarks. We will be prepared to go straight into evidence. But this is an evidentiary hearing that is in support of the motion to suppress the evidence obtained pursuant to the geofence warrant, and that is ECF 29, for which there has been a lot of subsequent briefing.

THE COURT: Now, you definitely can't speak that quickly, and I didn't hear at all what you said at the end.

MS. KOENIG: Sorry. For which there has been a lot of subsequent briefing.

THE COURT: Right. Okay.

So while we're waiting also, I want you to know we've gone through a lot of COVID protocol together. I can see that you all have been very mindful of it and will continue to be. I'm going to ask you to continue to be, certainly, all through this process.

We have a jury trial going on in a courtroom on this floor. And so what I want you all to do is not move in the hallways unless someone has allowed you to do it. We're trying to make sure that traffic is not congested so that, I guess, we don't lead into COVID congestion.

We can only do two people in an elevator at any one time. And we really are coordinating on the sixth floor, and a little bit on the seventh floor, with how we're moving people around. So, certainly, if you have any witnesses who are not in the courtroom, be sure they know that, too. Our biggest issues with COVID have been, understandably probably,

I don't want to the say anything too negative, but bored witnesses waiting for their time to be called and then sort of wandering around. And we just can't have that. So I'll appreciate your indulgence in that, too.

This is our simplest technology. I have never had an AT&T conference call not work. My apologies. They are only hearing us in binary language of beeps. I guess we need an interpreter. (

(IT is here now.)

THE CLERK: You can tell your folks they might have to call in again.

OPERATOR: Welcome to AT&T's teleconference service. Please enter your access code followed by the pound sign. There are 12 participants on the call including you.

MR. PRICE: I'm just letting them to know to call back.

THE CLERK: Okay. Can the people on the call hear us? Can somebody say something?

AN UNIDENTIFIED PERSON: Yes, we can hear you.

THE COURT: Thank you all.

All right. I understand now that folks who have called in on the AT&T line can hear us. We've

had some introductory scheduling issues taken care of about witnesses and presentation of evidence.

I also informed folks here, and I'm going to inform folks listening in on the AT&T line, that our Local Criminal Rule 53 and our standing order prohibits any kind of broadcasting or telecasting or recording of these events. Of course, you're welcome to listen in, but it is just as if you were in the courtroom itself.

We have one court reporter, who is making the single record that we will have of this proceeding. And it is a violation of our rules to in any way make a different or separate recording or record.

Can everybody hear me say that? Is there anybody on the AT&T call?

UNIDENTIFIED PERSON: Yes.

THE COURT: All right. So you all are on notice as to that?

UNIDENTIFIED PERSON: Yes.

THE COURT: All right. Okay.

So I will allow the defense to begin presenting evidence. I guess I want to confirm, is this a continuation of evidence that we heard with respect to discovery, the request for discovery, or is this a whole new record?

MR. PRICE: Your Honor, we will be repeating some of what we did in the discovery hearing but not all of it, so it's a continuation. There will be a little bit of repetition, but hopefully not too much.

THE COURT: Right. That's fine. I just want to make sure that both sides -- is the government in agreement that you're actually referring to both hearings as far as the evidence that I'm taking into consideration?

MR. SIMON: Judge, I think we asked that the Court certainly can consider that, but the record on appeal, I think, in this case will be about the evidence received at this particular hearing. And so we don't necessarily think that the transcript from the discovery hearing should override or overtake anything today. So we'd say focus on the evidence received here today, including from their expert Spencer McInvaille. But, you know, both sides may refer back to that testimony.

THE COURT: Well, that's my question. I don't want disputes about what I can take into account or what I can't take into account. You've been agreeing about the important issues, but it's easier to sort of set the parameters from the start rather than not.

MS. KOENIG: Sure. Your Honor, from the defense perspective, we have learned a lot of information from the time of today past January 2020. So to some extent, some of the issues that we talked about before, like some of the exhibits that we have on our exhibit list that we intend to introduce today, we took to heart the Court's direction that we shouldn't rely on past exhibits. So we are going to be referring and admitting those separately today.

There may be a couple of points that we may not spend as much time on, like, for example, the three paths video we spent quite a bit of time at the discovery hearing on. And we may not go too much in depth on that simply just to save time because we have a lot of witnesses and a lot of material to move through. But to the extent there is something different or contradictory or something that is changed, of course, today's record would control simply because at least the defense has moved well beyond where we were information-wise from January 2020.

THE COURT: Right. Which in part is -- although we've had, for lots of technological reasons and pandemic reasons and making sure we can have witnesses come in person from other places, we've had

delay, but we've also had delay that I think maybe will have available to us a better record.

What I'm going to say is that I want you all at the end of today, presuming we go into tomorrow, just meet and get a sense if there's going to be any dispute about what we can turn back to. And if you all want me to make any kind of speedy trial findings, I can do so now. Is that a good way to start or is anybody objecting to the delay that we've had? It's been pretty well documented through our case, and, in fact, Mr. Chatrie has asked for a couple of delays himself.

I think we've all been on the same page with respect to it, but if there should be findings on the record, I'm happy to make them.

MS. KOENIG: I think all the findings have already been made as to that, Your Honor, and we're just here today ready to move forward. The defense doesn't have any objections to the findings the Court has previously made.

THE COURT: Right. Okay.

Mr. Simon, you're in agreement?

MR. SIMON: Yes, Judge. And I don't think the Court was asking, again, about the record piece; is that right?

THE COURT: I'm sorry?

MR. SIMON: You weren't asking, again, Judge, about our review of the record, what the Court should consider?

THE COURT: No. I think you guys are going to agree. I just want to anticipate before anything gets too old in our minds any piece of evidence that you all think you may disagree about, we'll have a hearing on that, about what to do about it, and we'll do it now, not in two months, is what I'm saying.

MR. SIMON: Understood, Judge. And like defense counsel know, concerns about the delay here.

THE COURT: Okay. Thank you.

All right. So we're ready for the defense to begin.

MR. PRICE: Good morning, Your Honor.

THE COURT: Good morning.

MR. PRICE: Michael Price for Okello Chatrie. The defense would like to call Spencer McInvaille, please.

SPENCER MCINVAILLE, called by the defendant, first being duly sworn, testified as follows:

THE COURT: All right. Now, as you're approaching the podium and the witness stand, you all

may do whatever you wish with respect to your comfort zone with respect to COVID. You may take your mask off as long as nobody here in this room objects. We do have these plastic barriers. We have the sanitizing wipes and hand sanitizer.

The only thing I would say is certainly every time you leave any space, clean it off so that if somebody else goes near it or sits there also, it is fresh for them. We try to follow-up on that, too.

THE WITNESS: Yes, ma'am.

THE COURT: All right.

BY MR. PRICE:

Q Good morning, Mr. McInvaille. How are you?

A Good morning.

Q Would you please state your full name for the record.

A Spencer McInvaille.

Q And can you tell us who you are?

A Yeah. I'm a digital forensic examiner with Envista Forensics. I deal with cell phone location, location evidence in general. And I consult with prosecutors, attorneys, and defense counsel on those types of issues.

Q Thank you. And you've been previously qualified as an expert in this case in the fields of digital

forensic examinations, global forensics, and cellular location analysis?

A Yes, that's correct.

Q So I want to start with some basics.

THE COURT: So, Mr. Price, I'm going to ask you to move the microphone a little closer to you.

And also, Mr. McInvaille, if you could speak into the microphone. That's the way my court reporter hears you. She's not listening to you anywhere other than from her earphones.

And I just want to confirm the government has no objection to Mr. McInvaille testifying as an expert; is that correct?

MR. DUFFEY: We do not, Judge. Thank you.

BY MR. PRICE:

Q So I want to start with some basics here. And I want to ask you what sources of location data does Google use to locate phones generally?

A Sure. So for locating devices, you're generally going to see GPS data, Wi-Fi locations, Bluetooth locations, and cellular. Those are the main ways that Google would locate a device.

Q Can you explain each of those just a little bit? What's GPS?

A Sure. GPS is our Global Positioning System using

satellites to locate devices. People commonly associate that with how they navigate around town or go places with their phone.

As far as Wi-Fi goes, Wi-Fi access points are points on earth that we use to use data and things on our phones. As they capture where those are on earth based on signal strengths from each of those points, you can relatively locate a device as it pertains to how close it is to a certain access point.

As far as cellular goes, similar principle there. We know where the cell towers are. They communicate with a device. And based on signal strengths, you can determine where the device is in relation to the cell phone tower.

Q Are there any other sources of location data besides the ones that you mentioned?

THE COURT: So, Mr. Price, you're talking really fast.

BY MR. PRICE:

Q Are there any other sources of location data other than GPS, Bluetooth, cellular, and Wi-Fi?

A You can also use, say, IP addresses, too, to locate -- to generally locate someone.

Q How accurate are these sources? Maybe you can just talk about each one a little bit.

A Sure. They're going to vary. Cell phone towers, of course, cover very large areas. There are sectors. Each of them cover large areas. While they can, again, generally locate a device, they may not be the most accurate, but they can give us a relative location on earth.

Wi-Fi. Wi-Fi only extends so far. So it is going to give you a smaller area than what the cell tower probably could.

GPS can be very accurate. We can see that. It can be very accurate. Sub-meter accuracy at times with open skies.

THE COURT: Sub-meter or some meter?

THE WITNESS: Sub-meter.

THE COURT: Thank you.

THE WITNESS: Smaller than 1 meter.

So each has their own capability of how accurately you can place someone on earth or place a device on earth.

Q So when Google is using location information to find a phone, does it matter if someone is inside? Does it still work?

A No, it can still locate.

Q It still locates people inside or outside?

A Yes.

Q What are the -- what does Google do with this data? What are the repositories of location data that Google keeps?

A Sure. From my research, they keep this type of data in several ways. So you have Location History being that, as has been described, this journal of location history for a user. That can include each of those sources that we discussed on how information is gathered. And so it associates those with date and times for the device.

There's also Google Location Accuracy, which keeps up with some of that information we've talked about before with the access points, where they are on earth, how they make calculations, to make comparisons.

THE COURT: Did you say Location Accuracy?

THE WITNESS: Yes, ma'am.

THE COURT: Okay.

I'll let you say that again. I interrupted.

THE WITNESS: That's okay.

A As far as Google, there's Location History. There is Google Location Accuracy, as well as Web & App Activity also tracks IP addresses, and things like that, web activity application usage for general location.

THE COURT: Can you repeat what Location Accuracy is?

THE WITNESS: Sure. So Location Accuracy is going to -- is a repository of data as far as where access points and things like that are located so that it can be compared to other data for location purposes.

THE COURT: Thank you.

BY MR. PRICE:

Q So what does Google do with all of this location data?

A Sure. So this location data at this point, just data in general on people and their activities, is a lucrative -- it's a tangible item at this point. It's something that's used for advertising, understanding consumers and their habits, things like that. It's used for advertising, essentially.

Q The different kinds of advertising that Google does with this?

A Sure. So you have targeted ads from understanding what a person may want to -- you know, their interests. You can also target those ads based on their proximity to certain places. So if a particular business would like to try to generate more activity from the people that live and work around them, they

can try to target those people based on pushing ads to them because of their proximity to that location.

Q So if Google offers this advertising service to businesses based on location, do the businesses get the information about user location?

A Not to my knowledge. What the end user or the person paying for the advertising service receives is pretty much reporting on how well these ads are converting to revenue for them.

Q How would you explain the difference between targeting ads based on location and a law enforcement request for user location data?

A So as far as, again, with targeted ads for the business, the business is seeing whether or not their ads are becoming sales, whether or not people in the area that they're trying to pay -- they're paying to hopefully see these ads are coming to their business.

As far as in this law enforcement request or these geofence warrants, the difference is, is the return is different. The return is that you are seeing individual users, identifiers about those users, their location, and other information provided. So it's much different.

Q So just to clarify. What personally identifiable location information do businesses get when they do

this targeting?
A None that I'm aware of.
Q So we'll start with an easy one. What's a geofence warrant?
A So, a geofence warrant is a request by law enforcement to, in this case Google, to find out the users that are in a specific area. So a circle or box is drawn around a particular area where something happens. A time frame of that incident is also given. And the request is made to Google to find out who was inside of that particular area during the given time frame.
Q And did you review the geofence warrant in this case?
A Yes.
Q So what type of data was searched as a result of the geofence warrant in this case? Which repositories of data?
A So Google Location History was the searched area for Google.
Q Any others?
A No.
Q Who decided what kind of information was going to get searched?
A From my understanding, Google made the

determination to search Google history -- Location History, I'm sorry.

Q So there are three kinds. Google searched one and it was up to them?

A From my understanding, yes.

Q Could you describe how a geofence warrant works, what the stages are, how it unfolds process-wise, just generally?

A Sure. So the warrant is broken up into three steps. Each of those steps gaining more information as you go. So the warrant will spell out each of these steps for the process.

So, in Stage 1, a request is made for the geofence. So wherever the place is on earth. In this instance, it was a 150-meter circle, radius circle, that was drawn around a fixed point. And so the Stage 1 request is what users were inside of the circle during a one-hour time period.

Q And does it end there?

A No. So it goes further into each of the steps. So when that request is made, Google will respond with the location of the users and an identifier for each of the users who were inside of the circle at that time. So that's the steps from asking for Stage 1 to the return of Stage 1. Return of Stage 1 being a

spreadsheet of device IDs, locations, and the dates and times of those locations.

So once you have that information, you move into Step 2. Step 2 requires that a determination be made of how many of those users you want to know more information about. In Step 2, what Step 2 allows is contextual data. So it removes the geographical limits as well as the time frame expands. So you get more information about the movements of the people chosen out of Stage 1 about where they moved before and after the original geofence. You end up with that group of people. And now you know where they came from before the incident and then after.

Another determination needs to be made, and that's Step 3. Step 3, when you make that request to Google, you're asking for all of the subscriber information or all of the account information for the users that you've selected.

So in each step, you have -- you've made the large search of all users. Then you move into Stage 2 of a defined group out of that that you received. And then Step 3, again, another group that you've defined out of that to finally understand and reveal who those people are.

Q Thank you. I want to turn to the geofence warrant

in this case. Specifically, I'd like to call your attention to what's been marked Defense Exhibit 1.

THE COURT: So the record is clear, Exhibit 1 is being shown on the screens here in the courtroom.

Q Can you tell us what Exhibit 1 is, Mr. McInvaille?

A This is the affidavit for a search warrant in this case, the geofence warrant.

Q And this is the geofence warrant you reviewed?

A Yes, that's correct.

Q Thank you.

MR. PRICE: I'd like to admit Exhibit 1 into evidence, Your Honor.

THE COURT: Any objection?

MR. DUFFEY: No objection, Judge.

THE COURT: It will be entered.

MR. PRICE: Thank you, Your Honor.

(Government's Exhibit No. 1 is admitted into evidence.)

BY MR. PRICE:

Q Okay. So you just explained how geofence warrants work generally. We're looking at the warrant in this case. What happened here? Tell us how this works.

A So, again, there's a three-step process outlined in this warrant, as well. Again, a Stage 1, Stage 2, and Stage 3. So here the -- there's a time frame for

May 20th of 2019.

THE COURT: You have to talk about where you're referring to on the piece of paper because anybody reading this record is not going to have the document in front of them.

THE WITNESS: Yes, ma'am. I'm under Attachment 2 of the search warrant.

A So it defines the time frame that's going to be searched. So it's May 20th of 2019 from 16:20 hours until, on the same date, 17:20 hours. So a one-hour time period.

There's also a geofence drawn around a particular location. So they provide a latitude and longitude of where they're going to draw this radius. That radius was 150 meters. So the Stage 1 of that request was for users located within that circle during that time frame.

THE COURT: Now I'm going to interrupt you because it's my job to make sure the record is clear. In Defense Exhibit 1, I have a document behind a signed warrant that says Attachment 1, the place, person or thing to be searched. That has Roman numeral -- not Roman numeral. A numeral 1 at the bottom. And then the document I think you're showing me, there's a version of it that has a page 2. I'm

trying to find what you're actually showing me in Exhibit 1.

THE WITNESS: I'm on Attachment 2.

THE COURT: Got it.

THE WITNESS: And it's pages 2 and 3 at the bottom.

THE COURT: My apologies.

THE WITNESS: No problem.

THE COURT: I'm with you now.

BY MR. PRICE:

Q Okay. So what happened at Stage 1 here, specifically?

A So Stage 1 was a request for all Google users for that specific location. So within that circle during the hour time frame on May 20th.

Q And what did Google have to do to produce that information?

A So from what Google has told us, they require the search of all Location History accounts to complete that search to find out who was inside of that circle.

Q Do you know how many that was?

A They stated it was numerous tens of millions of accounts.

THE COURT: When did they say that?

THE WITNESS: That was in, I believe, Mr.

McGriff's declaration.

THE COURT: I think it's Marlo McGriff.

THE WITNESS: That's correct.

MR. PRICE: We'll come back to it, Your Honor.

THE COURT: All right.

BY MR. PRICE:

Q So after conducting a search of every Google user with Location History enabled, how many users were then sent back to law enforcement?

A Sure. So as a return for Stage 1, 19 unique identifiers were provided with location information for that one-hour time frame.

Q Thank you. And what happened after that? What happened in Stage 2?

A So a Stage 2 request was made to Google. Initially, a request for contextual data for all 19 were made. I believe that request was made more than once. And Google responded saying that that number needed to be reduced before they could respond to the Stage 2 request for contextual data.

That number was reduced to, I believe, nine. So nine users had contextual data provided. So that was the data that provides you 30 minutes before the initial time frame and 30 minutes after. So now our

time frame has expanded to two hours where there are no geographical limits during Stage 2 so that you can see movement before and after and outside of the original geofence.

Q Thank you. And then what happened in Stage 3?

A So Stage 3, again, a request was made by law enforcement for the Stage 3 request. In that request, they identified three users to reveal account information for.

Q Thank you very much. I would like to show you a slide from the report prepared by the FBI's Cellular Analysis Survey Team, the CAST team, and it's marked as Government's Exhibit 1. I'd like to show you page 8. Can you tell us what we're looking at here?

A So this is a similar picture to what you see from page 3 of attachment to --

THE COURT: Can we just go through the formality? Does the government object to this being placed in evidence since we're taking evidence from it?

MR. DUFFEY: We do not, Judge. It's our exhibit. So no objection.

THE COURT: Okay. So Government Exhibit 1 will be in evidence.

MR. PRICE: Thank you, Your Honor.

(Government's Exhibit No. 1 is admitted into evidence.)

BY MR. PRICE:

Q Sorry. What are we looking at here?

A So this is a similar picture to what is displayed in the search warrant on attachment to page 3. It shows the actual geofence. So that's the large red circle here. The point in the middle is the reference point that they provided to draw that radius from. And then you see the area that's encompassed by the geofence.

Q What are the places immediately implicated by this geofence?

A Sure. So you have the Call Federal Bank. You also have the Journey Christian Church. There's the parking lot for the church and bank, and then some of the wooded area surrounding both of those.

Q Thank you. Can we go to the next slide, please. So this is the next slide. Can you tell me what places are right outside the geofence as drawn?

A Sure. Special Agent -- he was able to identify some of these. And so you can, from his chart here, you can see the apartments. There's two different sets of apartment complexes here. Again, the previously mentioned locations.

You have A.M. Davis, Inc., a company that's across the street from the church. You have the Hampton Inn Hotel, which is just outside the church's parking lot. There's restaurants as well as a mini storage facility there.

THE COURT: I'm just going to put on the record this is page 9 of the same report of Government's Exhibit 1.

Q Okay. I'd like you to take a look at Defense Exhibit 3. If we could bring that up.

MS. KOENIG: Your Honor, this is an exhibit that the Court had previously placed under seal. It is the raw data from what Google produced. And so I believe since we are broadcasting to a different courtroom, it may be best to look at the paper copies of this, but it is Defense Exhibit 3.

THE COURT: Is there any objection to that from the government?

MR. DUFFEY: No objection, Judge.

THE COURT: All right. This has been placed under seal because of the potentially identifying information that is within it. And so we will review this document under seal.

MR. PRICE: Thank you, Your Honor.

Q Can you tell us what is Defense Exhibit 3? What

are we looking at?
A Yes. So it's the Stage 1 return for the Google geofence. It's the letters from Google telling you what they provided as well as PDF versions of the Excel spreadsheets or CSVs that were from Google.
Q So just to clarify, this is the raw data returns from the geofence warrant?
A Yes. This is what you would use to look and see where one of these devices was on the map. It provides you with locations and information about what was requested in Stage 1.
Q Can we take a look at column A?
THE COURT: Okay. We have to move them into evidence.
MR. PRICE: Excuse me.
Q You reviewed this in preparation for your testimony?
A That's correct.
MR. PRICE: I'd like to move this into evidence as Defense Exhibit 3, please.
THE COURT: Right. Any objection?
MR. DUFFEY: No objection.
THE COURT: All right.
MR. PRICE: Thank you for reminding me.
(Defendant's Exhibit No. 3 is admitted into

evidence.)
Q Can we take a look at Column A, please.
A Yes.
Q What does it say at the top of Column A?
A Column A is defined as device ID.
Q What about Columns B and C?
A B and C provide us a date and time.
Q How about D and E?
A D and E are the estimated latitudes and longitudes for those records.
Q So tell me more about that. How do those estimated latitude/longitude points relate to the geofence warrant?
A Sure. So these specific points -- so latitude and longitude is a reference of a point on earth. And these are the points that fell within the red circle that we previously spoke about. So within the geofence.
Q So where that latitude/longitude point is determines whether it gets reported in the geofence warrant returns?
A That's correct. So if this point were to have fallen outside of the red circle, it would not be provided. If it falls within the red circle, it is provided.

Q Okay. Now, let's look at Column G. What's that column?
A That's the maps display radius in meters.
Q In that column, there are some numbers, right?
A Yes.
Q What are those numbers?
A That is the estimated radius. So from the estimated latitude and longitude, a circle is then drawn, a radius circle is drawn around that point, and that's the estimation that the device should be within that circle by the estimate.
THE COURT: Within the second circle, not the original circle?
THE WITNESS: Correct. This circle is drawn around the individual points for that specific user for that specific record.
BY MR. SIMON:
Q How does Google draw that display radius?
A It would -- I don't know how they come up with it.
Q How does it appear?
A Oh, it appears -- when you draw it on the map, it appears to be the estimated latitude and longitude point in one place with a circle drawn around that to show you the area that the phone could have been in or the device could have been in.

Q Google has talked about something called a confidence interval. What's a confidence interval?

THE COURT: So you cannot be showing exhibits you're not talking about.

MS. KOENIG: Your Honor, that's my fault. My screen is locked, and I can't get out. So if we could unlock my screen, potentially I could get out to the correct exhibit.

THE COURT: Okay.

THE CLERK: I don't have control of your screen.

MS. KOENIG: There's a little lock button on the screen, Your Honor, on the right-hand side, and I was able to change exhibits before that lock appeared.

THE CLERK: Where it says "no stream detected"?

MS. KOENIG: Right above where it says "no stream detected."

THE CLERK: That's been there all along.

THE COURT: I just want to be clear, this is still part of Government's Exhibit 1.

MS. KOENIG: Correct. I wasn't intending to go to this stage, Your Honor. I was trying to get to the next exhibit, but it is frozen. There we go. All right. Okay.

MR. PRICE: All set?

MS. KOENIG: Yes.

MR. SIMON: Okay. Sorry about that, Your Honor.

THE COURT: That's okay.

MS. KOENIG: We're down to one paralegal in the Federal Public Defender's Office. I'm serving double duty, and it is not my specialty.

THE COURT: Congratulations on having a paralegal.

MS. KOENIG: Fair enough.

BY MR. PRICE:

Q Google has talked about something called a confidence interval. Can you explain to us what a confidence interval is?

A Yes. So they described it -- when they estimate the point on earth, so the latitude and longitude, and once they draw that circle around that point, the display radius, they have a rating or a goal of being how confident they are that they made the correct estimation, and that's 68 percent is their goal in determining the location on earth.

Q So they're saying -- so just to clarify. They try to be -- rephrase that. Is that a probability that somebody is going to be in there or just a certainty?

A It's their goal to be correct 68 percent of the time by estimating this latitude/longitude and drawing a circle around it, and that the phone should be located or the device should be located within that circle.

THE COURT: At 68 percent?

THE WITNESS: Correct. That's the goal.

THE COURT: And you used a phrase "confidence integral"?

MR. PRICE: Interval.

THE COURT: You've just got to be a little more clear because your witness hasn't said it.

MR. PRICE: Sorry.

THE WITNESS: Yes. That was their description of their confidence interval in the --

THE COURT: Interval not integral?

THE WITNESS: Yes, interval. Sorry.

THE COURT: Okay. Thank you.

BY MR. PRICE:

Q Can you tell us what this confidence interval has to do with the geofence warrant? What does it mean for how the results come in?

A As far as the results, we have to look at where the point is referenced on earth, the maps display radius, and just understand that even though it

provides that radius where the device should be located, it doesn't mean that it's absolutely within that radius either.

Q So what does it do to the effective range of a geofence warrant?

A It could make it larger.

Q I want to show you another slide from the CAST report. This will be Slide No. 20, page 20, of that PDF.

THE COURT: So that's Government's Exhibit 1, page 20.

MR. PRICE: Thank you.

BY MR. PRICE:

Q Mr. McInvaille, what are we looking at here?

A So, again, the red circle is the original geofence drawn. Each of the pin drops that you see, the blue and the red, indicate that the two differences between either GPS points that were located or Wi-Fi points that were located for a user. I believe this is an aggregation of all of the people for the Stage 1 return shown on the map.

And each of the blue circles that you see are those display radiuses provided in the records for each of those points.

Q So what do those -- those blue circles, that's the

display radius?

A Yes. That's the estimation that Google has provided for where the device could be based on their estimate for that record.

Q What do they tell us about the effective range of the geofence in this case?

A Sure. So if you were looking at one of these circles that extends outside of the geofence, so there's a few that you see, you see the larger one, and then you also see the others that encompass the roadway to the right or to the north.

Since the device could be anywhere within that circle, if the estimated latitude and longitude is off enough that it places the device inside the circle, even though it was not, that device is now included in this return even though the device never actually traveled within the circle.

Q So I want to take a look at that big blue circle there. What is that?

A That's a -- I believe that was the largest display radius provided for one of the records in the Stage 1 return.

THE COURT: Do you believe it or it is?

THE WITNESS: It is.

Q And what was the display radius for that point?

A 387 meters.
Q How does that compare to the size of the radius for the geofence as drawn?
A You can see from the map that it's roughly twice if not just a little bit larger than the original red circle. So the geofence circle.
Q So the radius is about twice as large?
A Yes, if not just a little more than twice.
Q What about the area covered by that?
A As far as like the squared area?
Q Yes.
A It would be a much larger area when you talk about area. Just expanding that circle greatly increases the actual area that would be compassioned by that circle.
Q So I promised I wouldn't make you do math on the stand.
THE COURT: You know, you're talking to him, but we need to hear you. And so it is more formal --
MR. PRICE: You can't hear me?
THE COURT: I can't hear you.
MR. PRICE: I said I promised Mr. McInvaille I wouldn't make him do math on the stand on the fly.
BY MR. PRICE:
Q So I'm just going to say the area of the geofence

as drawn, did you calculate that at some point?
A I did.
Q And was it approximately 71,000 meters squared?
A That's correct.
Q And the area of the large blue circle, did you calculate that area at some point?
A I did. So the larger was, I recall, to be about 470,000 meters.
Q Thank you. And --
THE COURT: Can you repeat the first one, please. I'm sorry.
THE WITNESS: Ma'am?
THE COURT: The first, the regular geofence.
THE WITNESS: About 71,000 meters, I believe.
THE COURT: Okay.
BY MR. PRICE:
Q And how many times larger is 470,000 compared to 71,000?
A Roughly, I would say six times.
Q About six times?
A About six times.
Q So is it possible that these map display radiuses could create a false positive?
A Yes, if you mean could someone be outside of the original geofence and actually be returned as if they

were inside the geofence.
Q How would that work?
A So if you're traveling by this geofence and the estimation that is made is incorrect enough that -- let's just say you're driving down the road here and that your physical device is actually on --
THE COURT: How about you name the road?
THE WITNESS: I believe it's Price Club Drive.
A If you're on Price Club Drive driving past the geofence and you don't actually cross into it, if Google estimates your estimated latitude and longitude to be within the circle, then you would have been included in this return even though the device never traveled within the geofence.
THE COURT: Within the blue circle?
THE WITNESS: Within the red circle.
THE COURT: Okay.
BY MR. PRICE:
Q So a false positive here would be putting somebody inside the geofence that wasn't there. Is it possible to have a false negative? How would that work?
A Sure. So if you -- if the opposite occurred, if you were inside of the geofence, but the estimation was made that your latitude and longitude fell outside

of the circle, then you would have not been included.

THE COURT: Wait, wait, wait. So why don't you -- so you're saying that if you're inside the original geofence and the estimate is larger than, say, 150 meters, you wouldn't be reported?

THE WITNESS: So what causes you to be included is the estimated latitude and longitude. If you kind of leave off the display radiuses, those blue circles, at the moment and just think of the estimates of the point that's given, so the latitude and longitude, if that estimate falls within the geofence, you are included. If that estimate falls outside of the geofence, you are excluded.

So the false positive occurs when that estimate is incorrect but actually falls within the fence even though you weren't in the fence. The opposite, the false negative, occurs when the device is actually inside the geofence but the estimate made falls outside the geofence.

THE COURT: So I'm looking at Column G in the exhibit that's under seal. In order to return a false negative, would G have to have a number above 150?

THE WITNESS: No, no. The false positives and negatives only occur due to D and F. Excuse me, D and E. The display radius is just the error radius

drawn around each point. The estimated latitude and longitude is what's critical in determining who will or will not be returned in the geofence originally.

THE COURT: So there's nothing in this exhibit, Defense Exhibit 3, that shows you an estimate that could fall outside, a false negative?

THE WITNESS: So if the false negative occurred, that means the device would have been inside the geofence. But by the estimate made by Google it fell outside the fence, so they were not returned in this, if that occurred.

THE COURT: G reflects the -- tell me what G reflects again.

THE WITNESS: G just reflects the blue circle that's drawn around these points. And all that is is the actual confidence that they place on the estimate. So if you see a point on the map with a very small circle, then they're giving you a smaller area that the device could have been in. A larger one, of course, is a larger area the device could have been in.

THE COURT: I thought it was reflecting the meters with which the confidence was expressed. That's not true?

THE WITNESS: I'm sorry?

THE COURT: I thought it was expressing the meters within which the confidence was expressed. So if it said 50, that it was within 50 meters of the longitude and latitude. That is not correct; is that right?

THE WITNESS: That is the estimation. That's what the display radius is for is to understand in relation to the estimated point of how far away the device should generally be from that estimate.

THE COURT: Right. So that -- maybe I'm going too far in depth, but if it's more than 150, if the estimate can't fall within 150 meters, it is not going to be reported because the geofence only goes to 150 meters.

THE WITNESS: Yes, but that reporting occurs because of D and F, not because of G. G is just a further piece of data that's given to us to understand the individual points.

THE COURT: Okay. I get it. No one else gets what I get, but I get it. So that's good.

MR. PRICE: I might give it one more try.

BY MR. PRICE:

Q Maybe we can run through a quick hypothetical here. All the blue and red points on this exhibit are inside that red line; right?

A That's correct. So they report it as being within the geofence, so they were returned.

Q If we suppose that there was somebody standing right outside of that red circle, maybe at the Ruby Tuesday Restaurant, and they had an error radius -- a delay radius of, say, 100 meters. Would that display radius intersect with the geofence warrant?

A It could, but that point wouldn't be returned. If that point is outside of the red circle, then it will not return within this stage of the request.

Q And it's also possible if we had somebody whose actual location was inside that geofence, but their radius extended outwards, it's possible that they might be outside that geofence? That they wouldn't actually be at their marker?

A It's possible. Like if you look at the point, it's kind of a long point up to the top edge of the red circle as you move north. As you see, that display, the point is within the circle, but the radius actually extends out just a touch over towards the Hampton Inn.

The phone actually or the device could be to the outer edge of that circle, which is outside of the geofence.

MR. PRICE: Does Your Honor have any

questions further on that point?

THE COURT: I will think about it, and I'll ask questions. We have Google folks coming.

MR. PRICE: Thank you, Your Honor.

BY MR. PRICE:

Q So if this big blue circle is the effective range of the geofence, can you tell us which places were encompassed by it?

A For this specific device, if that's where the device could be, you have -- again, you have the Price Club Drive, the road, you have Hull Street included, the Mini Price Storage, looks to be a few sets of apartments down here to the south and southeast side of it. The A.M. Davis, Inc., again, that we spoke about. Rockwood Village Apartments is the one I -- I can see it better now. So there's two sets of apartments there, as well, that are included.

So this device could have been anywhere around that location.

Q Thank you. I'm just going to switch gears here for a second. The government likens the geofence warrant to a tower dump in their briefing. Can you tell us, what's a tower dump? And would it have been useful here?

A A tower dump is a similar request. You don't

really know what you're asking for. You're making a request to the cell phone carriers for users, their subscribers, that are using towers in the area of, like, for instance, here, in the area of the bank. What they're going to return is spreadsheets that are going to tell you phone numbers that were using those towers that service that area.

The kind of point of all that is normally what you have is maybe one or two or more locations where incidents have happened over time. And what you're looking for as a result of these tower dumps is a common number or common numbers that show up in these records.

As a result of that, based on the process of elimination and the time of these incidents, if they're far enough apart and unique enough in time frames as far as small time frames, you would only expect if several incidents occur over a three-day period at different locations, that you -- if it's the same person, that you should only see one or two or a group of people working that specific thing. So it's a process of elimination that lets you understand when you don't have a suspect or an unknown group of suspects, it's meant to help you identify those people.

So that's a -- it's a request similar to this. We don't know what we're looking for. We just know that people have phones. So we're hoping that our suspect was using one and that he will be captured within those requests.

Q So would it have been useful in this case?

A It's difficult to say how useful it would be. You only have one location and date and time. So if you return back a thousand records, and you end up with a thousand phone numbers, you have nothing to compare it to, to really understand who in that group belongs there, lives there, works there, any of that, unless you know the phone number you're looking for.

Q Okay. Thank you.

Let's go back to the beginning of Stage 1. I think I asked you this earlier, but tell us how does Google know which devices are there?

A So within that geofence, again, it's a location on earth. They search the user's location history. So that repository of data of location history for their users and compare that latitude and longitude to see which users fit into that location. So broadly look at the data and pick out the ones that fall within that group.

Q So how did you learn about this?

A Through the declarations submitted by Google.

MR. PRICE: I'd like to pull up the first McGriff declaration, please. It's Defense Exhibit 21.

Q What is this document?

A It's the declaration of Marlo McGriff.

Q And did you review this in preparation for your testimony today?

A I have.

MR. PRICE: Your Honor, I'd like to move this into evidence, please.

THE COURT: Any objection?

MR. DUFFEY: No objection.

THE COURT: It will be entered.

(Defense Exhibit No. 21 is admitted into evidence.)

BY MR. PRICE:

Q So Google has to search through everybody in the Location History database. Do you know about how many people that is?

A They state numerous tens of millions.

Q I'd like to draw your attention to paragraph 13, please. Can you read for us paragraph 13?

A Yes. So, "In 2019, the majority of Google users worldwide did not have Location History, LH, enabled on their account. While a more precise percentage is

difficult to calculate in part due to fluctuating numbers of users in 2019, roughly one-third of active Google users (i.e., numbers tens of millions of Google users) had LH enabled on their accounts."

Q So to conduct the geofence search in this case, the government had Google search through everyone with Location History enabled and Google estimates that at numerous tens of millions of users?

A Correct.

Q In your experience, how does that number, numerous tens of millions, how does that compare to other types of warrants seeking location information?

A So, for -- you know, when we look at a request for call detail records for a single user, of course, that's a single user, normal Location History request for a specific account when they name the account because we know who we're looking at. Again, that's one user.

Probably the only thing comparable would be, say, the tower dump that you asked about earlier. But, again, as far as that number of people, it's not -- it wouldn't be close to that.

Q So, I want to turn your attention back to the CAST report. And this is Government's Exhibit 1 at page 13. Can you tell us what we're looking at here?

A Yes. This is the FBI CAST report, and there is -- you see the Sprint towers notated with the yellow kind of antenna sign. You have the Call Federal call out, so showing you where the bank is. You see the red circle for the geofence in there. And then a parameter is outlined with blue here, which they've -- which they've indicated as the estimated tower dump area had they conducted one with Sprint here.

Q So there wasn't a tower dump in this case, just to clarify?

A No. This looks to be a hypothetical of what that would look like if one was conducted.

Q How is this hypothetical set up?

A So it's showing you three towers that would -- that are in proximity to the credit union. Then you also see the geofence there and how it relates to those towers.

The blue appears to kind of indicate probably the estimated coverage that you would get from those three towers that are encompassed by the blue polygon. So what it's trying to show you is the area that would likely be affected had that request been made.

Q Would the government -- well, let me rephrase. Working with this hypothetical, in your experience, about how many people, how many users, would have

their records searched from a tower dump of just one of these towers?

A It's hard to say just because you're relying on how many people are using their device at the time, the number of people that you have in that area. I don't -- I have seen in past tower dump data sets a thousand users can be pulled for one of these towers.

Q So roughly a thousand for one tower?

A Possible.

Q And I guess if we're doing three, how many users would that be?

A Sure. If you kept that estimate, you'd be looking at, if you kept a thousand being what you think could be encompassed, it could be 3,000 based on three towers.

Q So 3,000 for the hypothetical here. How does that number compare to the numerous tens of millions in a geofence warrant?

A I don't know that it really does compare, but it's much less than numerous tens of millions.

Q I won't make you do any more math.

A Thank you.

Q I'll change gears here slightly. I want to ask you what this information tells you. What sort of information can you get from Location History data?

A From location?
Q Yeah.
A So with location for a specific person, you can learn a lot about a person. You can learn about their movements, the places that they frequent, places that they frequently travel or places they attend. So, for instance, when people have schedules, where they go to church on Wednesday. You could see if someone commonly goes to one of those particular locations, where they work, where they live, pretty much anything about daily life if you have enough points to look at.
Q How many is enough?
A How many?
Q How many is enough data points?
A You wouldn't need too many. You don't need days and days' worth of records. I mean, you can learn a little bit with just a small amount of data. You may not learn everything, but it doesn't take many data points to pick out a way of, you know, just a few locations, only one specific person could likely show up to each of those locations if you know the date and time that they were there. So it wouldn't take much data.
Q And how many data points do you think you might need to determine someone's identity?

A With just a handful, again, if you know if somebody shows up at four or five places in any given time, you know the date and time that they were there, pretty much you could learn something about that person.

Q So how do you know all this?

A I look at location data for a living. It's what I do. It's what I did prior to this job. I was in law enforcement and looked at data to try and get patterns for people's movements.

Q Have there been any studies written about this?

A Sure. I researched a few studies about Location History and how that information is gathered and used for ads and personalizing stuff to particular people.

Q I'd like to turn your attention to what's been marked as Defense Exhibit 9. Can you tell us what this is, please?

A Yes. That was a report written. It's called "Unique in the Crowd: The Privacy" -- I'm sorry. The "no stream detected" is blocking. It's an article about location and privacy. "The privacy bounds of human mobility" is the rest of it.

Q And this is a report that you reviewed in preparation for your testimony today?

A Yes, I've reviewed this.

MR. PRICE: Your Honor, I move to admit this into evidence.

THE COURT: Any objection?

MR. DUFFEY: Judge, I do object to this. I don't know what the relevance of moving an article in that he didn't write. He can testify about it, that he read it, and talk about it, I suppose. He's an expert. But to move the entire article into evidence as if we all agree it's all factually correct, I have no idea if it's correct. I don't know who the author is. I don't believe Mr. McInvaille knows the author. And so I object to it being moved wholesale into evidence. I don't object to him talking about it if he wants to talk about it. But that's my objection, is to relevance. And it's also quite clearly hearsay. I understand we're at a motion to suppress, and that's the Court's discretion on that. But I just don't understand the relevance of moving entire articles into evidence just because he read them. That's my objection.

MR. PRICE: Your Honor, Mr. McInvaille used these reports in the preparation of his reports. They are not being admitted for the truth of the matter even though we are under relaxed rules during our hearing here today. So we believe that it should be

in evidence. This is information that our expert relied on to draw his conclusions.

THE COURT: Well, I'm going to overrule the objection, but it's clear that we're not admitting it for the truth of what is in the article. It is a basis for the expert's testimony, and it cannot be admitted wholesale for the purpose of what the government is concerned about, which is that without any other testimony, we don't know anything about the study itself or how it was conducted. So it's really admitted as background information.

MR. PRICE: Thank you, Your Honor.

BY MR. PRICE:

Q Mr. McInvaille, can you tell us what your takeaway was from this report?

A Sure. The idea here is that just a few data points are revealing of a person's identity is the gist.

Q Do you remember how many were sufficient in this case?

A I believe they say four data points can tell you about a person.

Q So how long have you been working with location data?

A When I began working violent crimes. So probably

eight or nine years.
Q And in your experience, is that correct, the report's conclusion about the number of data points necessary on average to find somebody?
A I mean, it's -- not always is four points indicative of it, but yes, it can be. It depends on those points and what they tell you, but yes.
Q So, for instance, in this case, you previously created a video visualizing the geofence data for three users; is that correct?
A Yes, that was the Stage 2 return. So that contextual data for some of those users.
Q I'd like to show you what's been marked as Defense Exhibit 5. Is this the video you created?
A Yes.
Q Can you tell us what you did to create it?
A Yes. So, just using the latitude and longitude here so that you can understand the paths moving, again, there are display radiuses that go along with these, but this is more to just understand the general movement of these three devices and how they related from -- here what you see in the very beginning of each is where they fell within the geofence. And then as it moves along, it shows you where they were before, during, and then after the geofence for that

period of time.
Q Thank you.
MR. PRICE: Your Honor, I'd like to move this video into evidence.
THE COURT: No objection, is there?
MR. DUFFEY: No, Your Honor.
THE COURT: It's admitted.
(Defense Exhibit No. 5 is admitted into evidence.)
BY MR. PRICE:
Q Can we go ahead and play the video and have you describe slowly what is the happening here?
A Sure.
(Video is played.)
A So, again, you have the -- this is the initial return for this user. So the user ID is in the top left corner, and it shows you where they began in the warrant return.
THE COURT: I'm going to put on the record it's not identifying as to an individual; right? This is the Google number?
MR. PRICE: No, Your Honor. We previously -- that's a time stamp that you're looking at there. That's the number that you see. And for identification purposes, we've been referring to this

user or we had in the past as Mr. Green.

THE COURT: All right. Mr. Green. Got it.

A So in answering that question, the user here starts at this hospital here. And as you will see, they leave that location and travel south towards the geofence. You can see generally the path that they take, and as they travel south, it continues down to a residential area where it finally ends and the -- as far as the data goes that we were provided ends there in this residential area.

Q What does it tell you about what -- what do those cluster of dots over a house tell you?

A Sure. So you notice that those dots end up stopping at a given point. So here they kind of cluster around a house or a few houses here in this one area, meaning that the --

THE COURT: You're going to have to use phrases other than "in this one area," because we have a written record.

THE WITNESS: Sorry.

THE COURT: Because we have a written record.

THE WITNESS: Understood.

A So you see that the path had traveled down to this residential area here on the map. There is Decoy Lane is shown. So you see that it's at an address on Decoy

Lane or at least, you know, would be located very close in proximity to a few of these houses here on Decoy Lane.

Q Were you able to determine whose residence that is?

A I think you could. I looked at tax records and things like that for these houses in the area to take a look and see if based on knowing just the location, that you could possibly determine names for people there in that specific location.

Q I won't ask you to put the name on the record, but for Mr. Green, were you able to identify his likely identity?

A I was able to find some names for people from that residence for tax records. So, you know, I don't know that they are positively identified, but yes, there's information available for records for that area.

Q Would law enforcement have access to the same sort of information?

A Yes, this is publicly available information. You can search it on the internet.

Q Thank you. Can we resume the video and talk about Mr. Blue?

A So, again, blue -- starting here, this would have been the point that was returned for Stage 1 for that

device, and then we will see it move into the Stage 2 portion. So before, during, and after the geofence.

So you'll see to the bottom left here underneath the geofence there's the apartment complex just to the south. I don't recall the specific name of it, but it's just to the south off of Price Club Drive. So you see that the user's device is located in that complex and then begins to move outside of the complex up north to Hull Street before traveling some more.

THE COURT: Can you identify where it starts? You said it starts here in the geofence. What is that?

THE WITNESS: So the first point that was referenced from Stage 1 for that user, the point given, the estimated latitude and longitude, was there at the church, the Journey Christian Church.

Q Is that the first point in time or just the one that you got first?

A I believe that's the point that was given for that user for the Stage 1. And then now you're also seeing the Stage 2 portion of that.

Q So this user starts where?

A At the apartment complex just to the south of the geofence. So located along the southern side of Price Club Drive just south of the geofence.

Q And then what happens after he leaves his house? It looks like there's a point right inside the church.

A Yes. So you see that at some point during the video right here, it moves from several points that fall in the apartment complex and then begins to move outward as if it's moving from the apartments to Hull Street, which would, you know, the likely path would take you past the -- down Price Club Drive and past the geofence.

THE COURT: Past what?

THE WITNESS: The geofence.

BY MR. PRICE:

Q So, in other words, this may be an example of a false positive?

A It's possible.

Q Could you explain why?

A So, of course, you see the point there on top of the church which falls within the fence, which is how you get included. If this user was passing by and the estimate was incorrect, if we assume that they were driving down Price Club Drive and didn't enter the parking lot and only continued down the roadway, which was not included, if the estimate was incorrect and thought that the device actually did travel through the geofence, then this person was included even

though they did not pass through the geofence.

Q How would that happen in terms of the location data? Was this a Wi-Fi or a GPS point?

A I'm not sure, but it would be based off of a -- just due to the estimate, and its just inherent inability to perfectly place someone on earth.

Q So where does Mr. Blue wind up at the end of the day?

A Sure. So you see it travel south. It appears to travel to another residence in this area. I'm not sure of the road name here, but it ends up in this portion moving down to a more spread out residential area just south of where the geofence was and clusters around a single residence there before, I believe, moving back north again.

THE COURT: It's near the intersection of -- is it Alberta Road, counsel?

THE WITNESS: Yes, I see Albert Road. I was going to try to annotate it. Yeah, they're just south of where Alberta Road intersects with this other street.

MS. KOENIG: Your Honor, Mr. McInvaille can touch the screen and actually circle it so that it's clear for everybody.

THE COURT: It's three dots. The more we can

tie it to something, somebody else looking at it can find it, we need to do that. All right.

BY MR. PRICE:

Q So this is where the cluster ends for the records that we have?

A No, I believe it moves back north, but this is where they cluster for just a moment.

Q And would law enforcement be able to do anything with the information about the location of that residence? Would they be able to identify the likely residence?

A Yeah, it's possible this is clustered enough on that location that you would believe that that device did travel to that address. These are a little more -- these homes are a little more disbursed than the ones we spoke about on Decoy Lane. But, again, you could assume based on what you see here that that device traveled to that location. And, again, you can use publicly available information as well as law enforcement has other information at their disposal that, yeah, you could likely determine who would reside at that residence.

Q Thank you. All right. Can we resume play here and talk about Ms. Yellow?

A Yes. This is just the ending of what you see for

blue. Blue returns to the apartment complex located along Price Club Drive. Looks like Mallard Landing Circle, that area, is where it comes back to. That's where it started before it traveled to that residence we just spoke about and now it has returned there.

So you have yellow is displayed now. So yellow shows you the points that were given in Stage 1. Those points fall -- one falls just outside of the bank. Others fall on top of the bank.

So now it's moved to the point in time before the geofence. So we're again before everything, we're here at another residential area. These points seem to center around one residence, and then will eventually move as the data plays through.

THE COURT: Can you say where the residence is, what street?

THE WITNESS: Right around Buffalo Spring Drive. There's an intersection there. It's a residential home close to that intersection.

THE COURT: Okay.

BY MR. PRICE:

Q How many dots are sitting on top of one residence there?

A I'm not sure. It's a few. And then it moves north to a school that's up the road from the

residence. The school is located along Bailey's Bridge Road. So after what appears to be a stop at the school, it continues north to where you finally see this device inside the geofence.

After the geofence, it moves out of the geofence up Hull Street to some of the business area there before returning back to that same residential area from where it started.

Q So based on this information, were you able to identify Ms. Yellow?

A To an extent. I was able to see who owned the home that those points clustered around. And also just doing research into those names learned some more information about those people that's consistent with what you see in some of that contextual video.

Q Were you able to find social media about that individual?

A Yes. So the -- looking at -- looking for just publicly available social media stuff for the people listed for that residence that the data clustered around, you could also see that they had a school-aged child, that they were just recently married. So you could learn a little bit. You see that the school was possibly -- you know, that a stop was made at the school. So it coincides with just some of the readily

available information.

Q And the key for you here was which dots?

A So, again, the residential dots, the residence tells you, hey, there's, you know, that this may be the specific location because they're so clustered in that area, that that's the likely location, as well as the school, the school being another reference point just to understand something about someone. Of course you saw the bank, as well. The bank's the center of this.

So there was, you know, three locations there. Then if you look, some of those other businesses could have been traveled to as well in that area after the bank before traveling back home. So there's a few locations within that that could be telling of a person.

Q So the most important ones for you, though, were which in ascertaining Ms. Yellow's identity?

A If you were going to try and figure out who that person is, the home, the bank, and the school would be probably the most beneficial locations.

Q So three points?

A Sure.

Q And would this data be as identifying to you -- identifiable to law enforcement as it was to you?

A Sure. I mean anybody that could take a look at some of this data could learn something from it.
Q They would have access to the same tax records that you had access to?
A Yes, that's publicly available.
Q And social media?
A Yes.

THE COURT: I'm going to interrupt you. I know I asked you not to repeat too much, but is it the case that an earlier version of this video had lines about where the folks went in realtime or not?

THE WITNESS: No, I don't know the specific path. You can kind of understand the path, but no, I couldn't pick out the individual paths.

THE COURT: Fine. Just making sure.

BY MR. PRICE:
Q That's all we have on this exhibit. I want to shift gears a little bit now and talk to you about the opt-in method or Location History.

THE COURT: All right. So I'm actually going to take a break. We've been here awhile. Folks need to stretch. I have that it's 11:06. I'll give us 15 minutes. And so that would be 11:21.

You, sir, of course, will remain under oath, and you can't talk to anybody about your testimony,

nor can any other witness. And we'll come back and hit this new topic in 15 minutes. All right?

MR. PRICE: Thank you, Your Honor.

THE COURT: Okay.

(Recess taken from 11:06 a.m. to 11:21 a.m.)

THE COURT: All right, sir. Obviously, you're still under oath, and we'll continue your testimony.

I should probably do this every time in case other folks have joined. If anybody is here on the AT&T line, we welcome you. I need to remind you that our local rule, Criminal Rule 53, and our standing order prohibits anybody from recording or broadcasting or telecasting this proceeding in any way. We have a court reporter here who is creating what will be the official court record.

BY MR. PRICE:

Q All right. Mr. McInvaille, I want to talk with you a little bit about the opt-in method for Location History in this case. As a part of your work in this case, you reviewed the declarations of Marlo McGriff?

A That's correct.

Q I'd like to show you what's been marked as Defense Exhibit 23. Can you tell us what this is?

A Yes. This is labeled the "Third Declaration of

Marlo McGriff."

Q And you reviewed it in preparation for your testimony today?

A I have.

MR. PRICE: I would move to admit this into evidence, Your Honor.

MR. DUFFEY: No objection.

THE COURT: It will be admitted.

(Defense Exhibit No. 23 is admitted into evidence.)

BY MR. PRICE:

Q So do you know when Location History was first enabled on Mr. Chatrie's account?

A Based on this declaration, yes.

Q When was that and how do you know?

A It's indicated here. They provided the audit report from Google, which indicates when the -- when the activation of location or the enabling of Location History occurred. There are times listed on here.

Q And do you remember what time it was enabled on his account? I know we're having an issue here. There we go.

MS. KOENIG: Sorry. I'm getting there. Here we go.

A It was on July 9, 2018. And that was at 04:09

UTC. So in the a.m. for, of course, in UTC time zone.
Q What is UTC?
A UTC is a time standard. So it's just a thing that we reference time off of. It's used for many different types of records and everything, but, again, it's just a concept of time that we can reference local times off of.
Q So it was enabled at 4:09 UTC. I want to draw your attention to a line on page 2 of this declaration. It says -- can you read the highlighted part for us?
A Yes. So on this same page, Section C, "The user opted in to LH," Location History, "either through device settings or through a Google application on the Samsung device."
Q So can you translate that for us? What does that mean?
A Yes. So to enable Location History for an account to gather Location History for a device, you must enable Location History. And there's two prescribed ways of doing this. It's either through opening up the settings application on the device, logging in, and opting in to Location History through that method or when prompted through a supported Google application.

Q Could it have been enabled during the initial setup of the phone?
A Based on the time that Google is giving us, no, it would not have been enabled at setup.
Q Why not?
A Setup occurred July 2nd of 2018. This is, of course, July 9, 2018. So it was after the phone is setup.
Q Have you had an opportunity to examine Mr. Chatrie's cell phone in this case?
A I have.
Q And you produced a report detailing that examination; correct?
A I did.
Q I'd like to show you what's marked as Defense Exhibit 6. What is this?
A This is my report of the examination of the device.

MR. PRICE: Your Honor, I'd like to move this into evidence.

THE COURT: Any objection?

MR. DUFFEY: No, Your Honor.

THE COURT: All right. It will be entered.

MR. PRICE: Thank you, Your Honor.

(Defense Exhibit No. 6 is admitted into

evidence.)
BY MR. PRICE:
Q Can you tell us, Mr. McInvaille, how you examined the phone? What did you use to examine the phone?
A So I went to the FBI office and was given access to the device, and using Celebrite software I was able to download or extract the data from the device so that it could be examined.
Q Were you able to determine anything from that extraction about how Location History was first enabled?
A I was able to.
Q What did your determine?
A So, in my analysis, what I was looking for was activity that corresponded with the timing of what Google indicated was the activation or enabling of Location History. Through that, through my analysis of the data that I extracted, I was able to locate the installation of Google Assistant, which happened within just, I believe, a minute and a half or two minutes of just prior to Location History being enabled.
Q Can you tell us when exactly Assistant was installed? You said it was a couple minutes.
A Yes, I believe on UTC, it would have been 04:06

and some seconds, some milliseconds.
Q So it was about two minutes apart?
A Roughly, yes.
Q What else, if anything, was happening on the phone at that time?
A Based on my analysis, I didn't see much occurring during that time. If I recall correctly, the only thing very close in proximity to that was Google Assistant. I believe any activity prior to that was a few hours before, and then the -- I believe the only other Google application interaction that showed up around that time frame was, I believe, 12 hours later, if not more.
Q Did you -- I know this took you quite sometime. Did you look at anything else on the phone? How did you determine what else was going on on the phone at that time?
A So, to ensure that I feel I had adequately looked at all the data, Celebrite, what it does is it takes the data that's extracted --
THE COURT: Can you spell that for our court reporter who's not looking at your report, please.
THE WITNESS: Cellebrite, C-E-L-L-E-B-R-I-T-E.
A So using the physical analyzer software and

reviewing the data extracted, that software, what it attempts to do is take the data you have given it and turn it into something that we all can read.

So it parses that information out. Not always is every detail parsed because of changes in software supporting certainly applications and the level of detail. Oftentimes, you can look deeper into that data into the databases to find other artifacts that could be helpful. Dates and times, locations, just bits of information that can give you a better understanding of what it is you're looking at. So I also try to look into that to see if I can locate anything further that maybe wasn't readily available.

Again, my conclusion was that Google Assistant was pretty much the only thing that I could find that was occurring on the device during that time period.

Q You were able to find evidence of -- what were you able to find evidence of during that time?

A That the application was installed to the device at that time.

Q And you said you were able to draw a conclusion about how Mr. Chatrie likely enabled Location History?

A That's correct. So based on my understanding of Google Assistant, Location History, and this extraction, with those items occurring, so the

installation of the application occurring, as well as the activation of Location History just a minute or so after that, knowing that through the initial setup of certain applications through Google that they will prompt you to enable Location History, it's my conclusion that that is what would have activated or been the method of activating Location History at that time.

Q Thank you. So I want to talk about what that opt-in screen would have looked like in Assistant. And I'll turn your attention to the setup process for Google Assistant. Can you explain in a little more detail how that works?

A So when you -- when the application is on the device, generally people will activate that application by long pressing the home button. It's meant to be a convenience feature. So it opens the application.

During most applications, upon first use of really any application, there are certain things you have to do to set those applications up so that you can use them; preferences, permissions, those types of things.

So those would be things that would be prompted to the user as you begin to use your app for the first time.

Q Why is that process important in this case?
A Well, in this case, the reason that it's important is, of course, the only way that you are captured in this warrant that we have here is to have Location History enabled. So that function is critical in all of this. So without it, you will not be found within the warrant. So knowing if Location History is on or off, when it was activated, those things are important in this matter.
Q Did you attempt to determine what Mr. Chatrie likely saw when he set up Google Assistant for the first time?
A Yes, I've tried to understand that, you know, the 2018 method of opt-in procedures.
Q You actually prepared a supplemental report all about this?
A Yes.
MR. PRICE: Can we bring up Defense Exhibit 7.
BY MR. PRICE:
Q What is this?
A This is the supplemental report that discusses the opt-in.
MR. PRICE: Your Honor, I'd like to move this into evidence.

THE COURT: Any objection?

MR. DUFFEY: This is Exhibit 7?

THE COURT: Exhibit 7, yes.

MR. DUFFEY: No objection.

THE COURT: It will be entered.

(Defense Exhibit No. 7 is admitted into evidence.)

BY MR. PRICE:

Q So tell us, how did you learn about this process and what did you do first?

A So I looked at Android devices to try and get an understanding of what that procedure would be. The issue with trying to recreate some of these things is that software changes over time. Those updates when you're setting up these devices often automatically happen if you have them connected to Wi-Fi, which is kind of a critical piece of actually setting up the device as a normal person would.

So it kind of left me with the inability to see the 2018 or a confident way of knowing that back in 2018 this is what it would have looked like. So instead of being able to recreate, I turned to try and find information contemporaneous to that time to help me understand what that would have looked like at that time.

Q So you tried to recreate it, but that didn't work?
A Yeah, they just -- it looks different. The setup process is different than what it was. There's features that are different. It's just not the -- from what I see from research and then trying to recreate it, they don't look the same, and I didn't feel it would be an accurate representation.
Q Does it matter which phone you try and do this on?
A No. From everything that I know about this is that the Android, and across the devices generally, should be the same as far as this portion of the setup.
Q So unable to re-create it, what did you do next?
A So that's when I turned to information that I could find that was more in that time period of people setting up these devices and showing what that information actually looked like in 2018 versus now.
Q And did you, through defense investigation, become aware of any other information?
A Yes. So there were several articles or studies that covered, you know, screenshots and different information that would help you understand what those setup procedures looked like for the phone or applications, things of that nature.
Q All right. So, let's talk about what you found.

Were any of those particularly helpful to you? Which ones?

A I referenced three of the items in my supplemental report. There was an article and then two studies that showed pictures of the screens as they set devices up. And based on the information that they provided, you could see that these were Android devices with similar, from our understanding, similar operating systems and things and also were around this relevant time period.

Q So what was the first article that you came cross that you found to be helpful?

A I don't know that it's the first. It's the first that I reference here. But it's from the Quartz. And the article talks about Location History as one of the -- as the topic of the article.

Q What is Quarts?

THE COURT: Spell it.

MR. PRICE: Q-u-a-r-t-z.

THE COURT: Thank you.

A They have editors and people who write articles. It seems to kind of pertain around technology and different items.

Q All right. I'd like to show you what's been marked as Defense Exhibit 48. What are we looking at

here?
A That appears to be that article. Yes, that's the article.
Q So this is the article where you got the screenshots from for your report?
A Yes, lower in the report, in the article. Yeah, it was the Google Assistant permissions screen that I found.
Q Thank you.
MR. PRICE: And I would like to move this into evidence, as well, Your Honor.
THE COURT: Any objection?
MR. DUFFEY: Judge, same objection as the other article. If they're moving in, I guess, not for the truth, then I don't know what the relevance would be.
THE COURT: I'm going to overrule it. It's the basis of his opinion.
MR. DUFFEY: For the record, our objection is as to relevance. The point of the article doesn't seem to me to be the opt-in process. I understand he's relied on some of it, and he's put that into his report, and he can certainly talk about it, but we object to the entire article. And I understand the Court's ruling.

THE COURT: All right. I'm going to make essentially the same ruling, which is that you can argue the weight of the evidence, certainly, and cross-examine the expert with respect to it, but because, at least in part, it served as the basis for his expertise, it is admissible to that degree.

MR. PRICE: Thank you, Your Honor.

(Government's Exhibit No. 48 is admitted into evidence.)

BY MR. PRICE:

Q So in addition to the Quartz screenshots, did you find any others? What was the next one that you cited in your report?

THE COURT: Now, wait a minute. Now, he said there is the Quartz screenshot right there in that article. Would you like to identify for the record where it is?

MR. PRICE: We will certainly try, Your Honor. I'm not sure that there are page numbers. It is on page 6 of the PDF itself.

THE COURT: Why don't you identify what's on -- like, does it say, for instance, Google Maps, Google app? That are words and headings that help.

MR. PRICE: There is a heading that says "Google Assistant." And there is a screenshot below

that which has a blue bar on top and says "Give your new assistant permission to help you."

THE COURT: Perfect. That's great. Thanks.

BY MR. PRICE:

Q Mr. McInvaille, so this is one of the screenshots that you believed might be similar to the one that the user would have seen in July of 2018?

A Yes, it's similar.

THE COURT: Why don't you just put on the record why. Is this article dated?

THE WITNESS: Yes, I believe January of 2018 was the date. The reason that it's similar is, again, you see a similar layout, give permission for your assistant to help you. Similar wording. There are some differences in some of them as they move along, but as far as the structure and the question that is being posed to the user, they are similar.

THE COURT: Similar to what?

MR. PRICE: I think we're going to try and compare the different screenshots here, Your Honor. So I just want to have all three so that we can talk about their similarities and differences.

THE COURT: Okay.

BY MR. PRICE:

Q But, Mr. McInvaille, can you please read what it

says there under "Location History," just so we have it?

A Sure. So on "Give your new assistant permission to help you" is the kind of header of this permission screen. It tells you the -- it will tell you the account that you're using as it's asking permission to activate certain things for that account.

And then you have Location History, device information, Voice & Audio Activity are the permissions that are being asked to be given. Each of those topics have their own description and expansion arrows.

Location History indicates that you're giving permission to -- it creates a private map of where you go with your signed in device.

Device information. It includes contacts, calendars, apps, music, battery life, and sensor readings.

And then voice and audio activity. Records your voice, audio input, to help recognize your voice and improve speech recognition.

Q Thank you. I'd like to move on and look at the next screenshot that you found that you included in your report. Which one was that?

A Sure. This is from a study from Oracle. Oracle

is a technology company, a computer science company, I believe. They show the Google Assistant process, but they also show the previous screen to what you see from the article that we just mentioned from Quartz.

So they're showing you both the initial screen that you see when you open Google Assistant for the first time to set it up, as well as the subsequent permission screen that we just discussed.

The information contained with those, besides the account, of course, because these are two different people setting this up, the other substance is the same here for these two screens.

So, first, you have "Meet your Google Assistant." It asks how it can help. And then you have to either skip that procedure and not completely set up or press "Next" to completely set up.

You press "Next," that's when it takes you to the permission screen that we just outlined prior to this. And so then you have another piece there at the bottom that was not covered because you couldn't read it, but the options that you have are "No, thanks" or "Yes, I'm in."

Q I'd like to show you --

THE COURT: Wait. Did you identify what document that came from, the Oracle?

MR. PRICE: That's what we're going to do right now.

THE COURT: Okay.

BY MR. PRICE:

Q Can you tell us what we're looking at here?

A Sure. So this is the cover page of the Oracle study. It's "Google's Advertising and" I believe that says "Data Dominance."

Q Is this the document where you got those screenshots from?

A That's correct.

Q You reviewed it in putting together your report?

A I did.

MR. PRICE: I'd like to move it into evidence, Your Honor.

THE COURT: What number is it?

MS. KOENIG: Sorry. This is Defense Exhibit 10.

MR. DUFFEY: Judge, same objection. I'd also point out Oracle is in protracted litigation with Google. They are adverse to Google. I guess that goes to the weight, but I'm still objecting to relevance, and I'm objecting to hearsay for the entire report to come in.

THE COURT: All right. Well, for the same

limited purpose, I am going to admit the exhibit. And you can argue the weight of the evidence, including you can cross-examine about the fact that Oracle is litigating against Google for perhaps a bias of the report. All of that can be part of the record. And then it will be introduced for that limited purpose.

(Defense Exhibit No. 10 is admitted into evidence.)

THE COURT: So, Mr. Price, I'm going to tell you, for us who don't know what you're doing, if you're showing a screenshot, you're really having the witness testify from something that's not in evidence yet. So unless you refer to where the screenshot is in the report, so we know where you got it from, it would be not proper for him to be testifying from the Oracle document yet.

So if you say what part of the page of the report that you're using the screenshot, that helps those of us who don't know in advance what you're doing to understand what you're doing.

I was presuming, I'll tell you, that that screenshot was from this report, and it wasn't in evidence yet. So we just -- we're not with you. So you have to be -- you have to go granular into where these documents are coming from. Okay?

MR. PRICE: I will, Your Honor.

Can we bring up the specific page in the report, please.

BY MR. PRICE:

Q Mr. McInvaille, you don't happen to remember which page it was on, do you?

A I don't.

MR. PRICE: Apologies for the delay, Your Honor.

We are going to move to withdraw Exhibit 10. And we'd like to show Mr. McInvaille Defense Exhibit 11.

THE COURT: So Exhibit 10 is withdrawn. I want to be clear. Your exhibit list indicates that that's a June 2018 Oracle submission. And so maybe also referring to it by date would be helpful.

MR. PRICE: Yes, Your Honor. We are referring to the September 2018 Oracle submission. Apologies for the confusion.

BY MR. PRICE:

Q I'm now showing you what's been marked as Defense Exhibit 11. Can you tell us what this is?

A Yes. This is the correct exhibit for the screenshot that I show in my report.

Q And what page of the Oracle submission does the

screenshot appear on?
A The page number that I have is four here. And it is -- the paragraph surrounding it starts with "Continuing through the Android smartphone setup process."
Q And this is where you got the screenshot for your report?
A That's correct, the screenshot that we're referring to in the report came from this section here.
Q Thank you.
MR. PRICE: Your Honor, I'd like to move this into evidence, Exhibit 11.
THE COURT: Mr. Duffey.
MR. DUFFEY: Same objection as before, Judge.
THE COURT: All right. I'm going to admit it for the limited purpose, not for the truth of the matter, with the government's concern for the weight, but as a basis for this expert's opinion, it will be admitted.
(Defense Exhibit No. 11 is admitted into evidence.)
BY MR. PRICE:
Q How does this screenshot compare to the one from Quartz that we just talked about?

A Yeah. So, again, this is -- it gives you the prior screen to the permission screen. So the "Meet your Google Assistant" screen where you can make two options of either "Skip" or "Next," "Next" being the one that takes you to the permission screen that we outlined previously with the different paragraphs or the different explanations.

Q Is there any difference in the text as far as you're aware?

A No. The Quartz article screenshot and this screenshot is consistent. They are consistent with each other as far as wording.

Q Okay. Thank you. I want to move on to that third set of screenshots that you found. And I want to show you Defense Exhibit 27. Can we look at your report, and can you show us that third set of screenshots? Can you tell us what these are?

A Yes. So another set of screenshots from a different study. This study is from the Norwegian Consumer Council. Again, taking you through kind of what the setup process looks like for Google Assistant. These were from the June time period of 2018.

Q Where did you get these from?

A The Norwegian Consumer Council. I don't know if

you consider it like Better Business Bureau. It's a consumer reporting agency. It's funded by the Norwegian Government to educate consumers on different products.

Q What did they do relevant to this case?

A Sure. So they're showing Google features as far as setup processes, requests, and permissions, and it resolves around data collection.

Q Do they publish anything?

A Yes, they publish a study on their findings in different data collected by Google.

Q So I would now like to show you what's been marked as Defense Exhibit 27. Is this the -- well, what is this?

A This is an article. It's titled "Every Step you take." I can't actually say the name of the Norwegian -- the name of their agency, but it's the -- they call it the Norwegian Consumer Council.

THE COURT: How about you spell it? It's on the diagram; right?

THE WITNESS: Bottom right of the page. It's F-O-R-B-R-U-K-E-R-R-A-D-E-T.

Q And this is the document where you got those screenshots from?

A Yes.

Q Can you tell us which page you found them on?
A Working on it. There is an -- it's page 19 of 44. It's titled or the header is "Enabling Google Assistant," and you see screenshots there for Google Assistant.
Q And you used these screenshots to prepare your report?
A Yes, I believe there's actually a section with more of those expanded.
THE COURT: Sir, did you say "I believe there's more explained"? Are you looking for more documents?
THE WITNESS: No. Inside the -- inside the document there's another section with, I believe, more screenshots just underlying the same thing. I pointed out one of the sections that had some of those screenshots in it. I was trying to make sure that I referenced all of the places where the --
THE COURT: So you haven't told us about the other ones yet.
THE WITNESS: Ma'am?
THE COURT: You haven't told us about the other ones yet?
THE WITNESS: No. I'm just trying to see where they were in the document, what page they were

on.

THE COURT: In the meantime, Mr. Price, are you moving this into evidence?

MR. PRICE: Yes, Your Honor.

THE COURT: Any objection?

MR. DUFFEY: Yes, Judge. Same objection as before, irrelevance under hearsay.

THE COURT: All right. I'm going to overrule for the same reasons.

(Government's Exhibit No. 27 is admitted into evidence.)

THE COURT: Can we just put on the record the date of this report? I think it's on the first page.

THE WITNESS: Yes. November 27, 2018.

THE COURT: Thank you.

BY MR. PRICE:

Q Did you receive any additional information from the --

THE COURT: He's still looking for pages. Right?

THE WITNESS: That question will answer that issue.

THE COURT: Okay.

BY MR. PRICE:

Q Have you reviewed any additional screenshots

provided by the Norwegian Consumer Council?
A Yes. In their report, you see the page that I referenced. I believe it was page 19. There were more screenshots available than what is just displayed on page 19. It expands upon some of these expansion arrows and just gives some more detail.
Q And you've seen those?
A I have.
Q Where did they come from?
A They were provided to me by counsel.
Q And they were what in relation to this report?
A So, they were the underlying information that the counsel used to create this. So it just -- it's more of the screenshots, more of the detailed shots that go along with this explanation.
Q And you reviewed those for your report?
A I did.
MR. PRICE: Can we pull up the third set of screenshots from your report?
BY MR. PRICE:
Q These are the screenshots you obtained directly from the Norwegian Consumer Council?
A Yes, that's where they were obtained from.
THE COURT: Do you want to refer to a page in the report and what exhibit number it is?

MR. PRICE: We are on page 5 of the supplemental report. So that would be Defense Exhibit 7.

THE COURT: Okay. Thank you.

BY MR. PRICE:

Q Can you tell us what these screenshots show us?

A Sure. Again, these are more screenshots for the setup for Google Assistant. These were helpful because they just give more information than those we saw in other articles. They expanded the expansion arrows. They are also, from what we understand from Google's declaration, a more accurate version of what we think would have been seen during the actual setup of this device that we're talking about today.

Q When are these screenshots from?

A These screenshots were -- I believe it was July 2. Yeah. Some were taken in August. Some were taken in July.

Q So there are two sets here, two sets of screenshots. One that we're looking at now on page 4?

A Yes. Page 4 is the July 2 screenshots.

Q And then we have one more set. When are those from?

A August 9. And those are on page 5, Figure 4.

Q So I want to go up to the July one. Can you tell

us how these screens differ from the Oracle and Quartz screens that we just talked about?

A So they look very similar as far as structure. Really, the only difference is some of the wording that you see as far as the descriptions of what permissions are being given. You're still provided with the same permission. So Location History, device information, Voice & Audio Activity, but the explanation underneath each of those or the explanations are different in these screenshots. And as I understand from Google submissions, these are the screens that the user would have seen during the setup of this device.

Q Can you remind us, for the record, when Location History was enabled?

A Location History in this case was July 9th of 2018. So a set of these were just before and another set was just after.

Q How did that affect your confidence in determining which one was the likely one that was in place at that time?

A Again, these are close in time to the time that we know Location History was enabled. And also Google has submitted saying these are the screens that the user would have seen at that time, as well. So that's

why I lend more confidence to these being the true depiction of the opt-in process.

Q Is the language on these screens consistent with the text in Mr. McGriff's affidavit?

A With Mr. McGriff's affidavit?

Q Yes.

THE COURT: Is it Mr. or Ms.? It's Marlo.

MR. PRICE: Mr.

THE COURT: Marlo is Mr.?

MR. PRICE: Yes.

THE COURT: My apologies. Okay. Thank you.

A Yes. So in Mr. McGriff's affidavit, he does show a portion of these screens or he doesn't show a screenshot, but the text from it. So the give your permission, Location History, what it says under Location History, which says "Saves where you go with your devices." And then also the little footnote just above the selections that you can make is included in his affidavit or declaration.

Q So we have the Quartz and Oracle screenshots that say one thing. And those are from when?

A As I recall, probably January of '18. That time frame is my understanding.

Q The beginning of 2018?

A Beginning of 2018.

Q And these are when relative to that?
A Mid 2018. July, August area.
Q The language changed between the Norwegian screenshots and the Oracle and Quartz screenshots. What does that tell you?
A That just tells me that Google made a change in how they display this information to the user.
Q Can we scroll down to the August screenshots. So there's a couple of buttons at the end there. What do those say?
A So, again, this screenshot is asking for permission. It says "Give your new assistant permission to help you." And then there are the three categories that you're providing permission for. And then at the very bottom you have the choices of either "No, thanks" or "Turn on."
Q Are the "No, thanks" and "Turn on," are those the same choices available in the Quartz and Oracle screenshots?
A No, I don't believe they're the same questions.
Q Instead it says -- looking at the Oracle one, what does it say?
A "No, thanks" is one, and "Yes, I'm in" is the other.
Q So that language there is different, as well?

A It is.
Q Tell me about the long press on an Android phone. What does that do?
A Sure. So the buttons on the front lower portion of the phone down where your thumb would normally be if you were holding the phone, kind of where you would speak into the phone, down there our phones now really don't have buttons on the screen anymore. Everything is touch screen. But in the center of an Android, or most Androids, you have a home button. What you can do is press, and it's called a long press. It's kind of a press and hold of that button to activate Google Assistant. So it will launch the application from that long press.
Q So if you press and hold the home button?
A Yes. It pops it up on the screen.
Q So, in your opinion, which set of screenshots is the likely one that Mr. Chatrie would have seen?
A Those that we see, as in Figure 4, here in the report from August, that or the others in the previous figure. Both of those are confirmed by Google as being the most likely screens that would have been seen by the user during this time period.
Q Did you have an opportunity to compare these screenshots with the screenshots that Mr. McGriff

provided in his declaration?
A Yes.
Q Those weren't for Google Assistant, though, were they?
A No, it was just a Location History permission request. I guess an opt-in screen for Location History.
Q So, can you tell us how these screenshots differ from the ones that Mr. McGriff provided in his affidavit?
A So, Mr. McGriff's is -- I wouldn't call it so much as a screenshot as it's just the plain text from what you would see in the screen. So, again, in the screenshots that we have here from these articles, they kind of show you what the user would see in kind of the way they would see as far as the screens. Mr. McGriff's just holds the text.
THE COURT: Mr. McGriff just what?
THE WITNESS: Just the text.
THE COURT: Okay.
THE WITNESS: Instead of the actual screen, like pictures, he's showing more of just the words that would have been displayed.
They're different just because in Mr. McGriff's, he doesn't show you each of the options

that are being given in some of these screenshots. He's only showing Location History and then that footnote that's provided underneath it, as well as what options there are for either "No, thanks" or "Turn on."

MR. PRICE: Perhaps we can pull up Mr. McGriff's affidavit.

Q This is the third affidavit, and it has previously been marked as Exhibit --

THE COURT: 23.

MR. PRICE: 23. Thank you.

Can we scroll down? All right.

BY MR. PRICE:

Q This is the text. What are we looking at here?

A Sure. So it shows that the opt-in screen would contain the following text: Location History.

It has the "Saves where you go with your devices" text that is consistent with the screenshots that we were just looking at. And then it also has, like, the kind of footnote paragraph that's just above the options that you have. So "This data may be saved and used in your Google service where you were signed in to give you more personalized experiences. You can see your data, delete it, and change your settings at account.google.com." Then you have also the "No,

thanks" and "Turn on" options there.
Q So in the actual screenshot, though, does the language appear that way visually?
A No. There's more in the screenshots of what the user would see. So, again, they're asking permission for Location History, as well as device information, Voice & Audio Activity. There are other descriptions and expansion areas. There's just more in the screenshots that the user sees than what's displayed there.
Q And that language you just read from Mr. McGriff's affidavit about how the data may be saved and used in any Google service, where does that appear relative the Location History prompt?
A It's down the page. It's at the very bottom of the screen where the options for the selections are.
Q How does it appear visually? Is it the same darkness as the other language on the page?
A Is it the same -- I'm sorry?
Q Font.
A I'm not sure. It does -- again, it's just the words from the page. It's not the actual screenshots. The screenshots that the user sees has different icon descriptions. It's visually different and has some content in the screenshots that's not in the

affidavit.

THE COURT: Okay. You're referring to the language in the affidavit, paragraph 7; correct? And now you've turned back to page 4 of Exhibit 7, which is your own report. Are you talking about Figure 4?

THE WITNESS: Yes, Figure 4, the picture to the right. What I'm referring to is that it contains more information than what's put into the bottom page of Mr. McGriff's declaration.

THE COURT: Okay.

BY MR. PRICE:

Q What do you mean by "more information" here?

A Well, there is a request for more than just Location History happening. There are more descriptions of those other permissions that are being requested. There are -- as well as expansion arrows to open up and see what else is available to read. It's just a little bit different than what you see in his affidavit.

THE COURT: So, specifically, it says -- on the right-hand part of the screen, it has -- it says "Location History," and it has an icon next to it, and a line under it; "Device information," and an icon next to it and a line under it; "Voice & Audio Activity," and an icon next to it and a line under it.

And then it has, not as a footnote, it says, "This data may be saved and used in any Google service where you are signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com"; correct? That's what you're testifying to.

THE WITNESS: Yes.

THE COURT: So there are two more subsections than what is reflected in paragraph 7 of the third McGriff declaration?

THE WITNESS: That's right. There's two other permissions that you're being asked to provide permission to.

THE COURT: Okay.

MR. PRICE: Thank you.

Can we bring up Mr. McGriff's affidavit one more time? I'd like to see the screenshots that he provides or maps.

BY MR. PRICE:

Q What are we looking at here?

A This is Mr. McGriff's declaration, page 7. These are screenshots from Google Maps.

THE COURT: This is Exhibit 23, McGriff Declaration 3, since there are three of them. We're looking at Exhibit 23; am I correct?

MR. PRICE: Yes, Your Honor. Twenty-three, page 7.

THE COURT: Okay.

BY MR. PRICE:

Q So, by comparison, comparing the Assistant setup screen and the Map setup screen, can you tell us along the lines of what you're saying, what is different between these two?

A These, again, appear differently. They're asking for similar permissions but appear differently. They actually have less permissions than what you're being requested from for Google Assistant. Location History is one of those. It has the drop down. It also has the line underneath it for "saves where you go with your devices." It also has the paragraph underneath it that's just above the "No, thanks" and "Turn on" buttons that you saw from previous requests but here now for Google Maps.

Q So there's one screen for maps, one set of permissions for Location History, and two options, "Turn on" or "No, thanks"?

A Correct.

MR. PRICE: Can we go back to Mr. McInvaille's report, supplemental report, Exhibit 7, page 5.

BY MR. PRICE:

Q By contrast here, how many permissions is Google asking for?

A For Assistant, it's askings for three permissions.

Q What are the options at the bottom?

A "No, thanks" and "Turn on."

Q Does that apply to Location History?

A Yes.

Q Does it apply to device information?

A It applies there, too.

Q Does it apply to Voice & Audio Activity?

A Yes. It applies to everything you see on the screen. The request is for all three of those items at once.

Q So what are the users options at that juncture?

A Either to turn it on or not turn it on.

Q Turn what on?

A Location History, device information, Voice & Audio Activity.

Q So either turn all three on or don't?

A Correct.

Q Those little upside down triangles, what are those on the screen there that we're talking about? There are three of them. One is next to Location History. One is next to device information. One is next to

Voice & Audio Activity.

A They were referred to in some of the -- in the declarations as expansion arrows. It just expands the area underneath each of those topics. And there's more information contained under each of those tabs.

Q I think we have that on the screen. If we can show the language.

We're on page 4 of Exhibit 7. Can you tell us what we're looking at now?

A Sure. These were included due to the expansion arrows actually being selected so that you can see the information underneath each of the permissions being given.

Q But that information is not visible from that first screen?

A No. Unless you click the arrow, you can't see all of the data.

Q Do you have to click the arrow?

A No, you don't have to click the arrow to make a determination of on or off.

Q So, I could enable Location History without ever clicking on that expansion arrow?

A Right. You don't have to see this to make a selection.

Q Does it say "learn more" or "more info" here?

A I don't recall any of these having that option.
Q What does Google say in the screenshot about whether Location History is necessary for Assistant to work?
A So the kind of, I guess, characterization that's put at the top is Assistant depends on these settings in order to work correctly. Turn these settings on for this account. It specifies the account that you're making that selection for. And then tells you what permissions you're acknowledging to make Assistant work correctly.
Q Can you set up Assistant this way?
THE COURT: Wait a minute. Where are you reading from?
MR. PRICE: Right under "Give your new Assistant permission to help you." It says -- it's the middle screenshot.
THE COURT: So you're on page 3. You moved to page 3?
MR. PRICE: I believe we're still on page 4. Three screenshots in a row. We're looking at the middle one.
MR. DUFFEY: Judge, I have page 3. So I'm a little confused.
THE COURT: Right. My page 3 has on the top

of it "Device Information" and on the bottom "Voice & Audio Activity." And my page 3 has "Location History. Saves where you go with your devices." And that's the one that has the "Meet your Google Assistant."

MR. PRICE: One moment, Your Honor. Your Honor, are you looking at Exhibit 7?

THE COURT: Yes.

MR. PRICE: Page 4?

THE COURT: I'm looking at page 3 and page 4.

MR. PRICE: We have it on the screen now. I'm not sure why your version -- page 3 has the Oracle screenshot. Page 4 has the one that we are looking at from the Norwegian Consumer Council.

THE WITNESS: The page number at the bottom is different than the PDF page number is what it is.

Q Okay. What page?

A Scroll down just a touch. So, the page number at the bottom right is 3.

Q Okay. My apologies.

So we're looking at page 3 of Exhibit 7, the Norwegian Consumer Council screenshots from July 2, 2018. And in the middle screen it says, "Give your new Assistant permission to help you." And then, sorry, can you read that language one more time?

A Yes. So, in that middle screenshot, "Give your

new Assistant permission to help you." Just underneath that, "The Assistant depends on these settings in order to work correctly. Turn on these settings for," and that's referring to what account you're turning the setting on for. And then it indicates what settings you are either turning on or not turning on.

Q Thank you. And if we're setting up Google Assistant in this way, and you want to turn it on, Assistant, what do you have to do?

A As they indicate for it to work correctly, you need to give permission to these -- to the permissions shown to the user.

Q You need to give permission for all three?

A Yes. You don't get to pick individually. It's all three.

Q So let me ask you, what would happen to Google Assistant if you disabled Location History later on?

A You could still use it.

Q It works?

A Yeah.

Q Even if Location History is not enabled?

A Yes. You don't need Location History for it to work.

Q So why would Google make it a requirement to set

up Assistant?
A I'm sorry?
Q Why would Google make it a requirement to start Google Assistant?
A I think they're asking for permission to make it better. Again, you don't have to use it, but it's a, as they say, for it to work correctly or as intended, the permissions help in that way.
Q But it works without Location History enabled?
A You can use it without Location History.
Q And where on here does Google tell us that?
A I'm not sure they do. I just know that you can use it without Location History being enabled.
Q Thank you. Switching gears slightly. I want to talk about Location History collection more generally. When does Google collect location history information?
A When the user -- if it's enabled by the user from everything that I have seen as far as data outputted from Location History, it's always collecting.
Q Always?
A Very consistently throughout the day.
Q What if the user is not using Assistant?
A It -- again, from seeing the times of day and things that are referenced in these records that we see from Location History, it appears to happen all

times of the day. So when the user is sleeping, not sleeping. It's a lot of information that's being gathered as far as just location is concerned.

Q What if a person isn't using an app at all on their phone?

A I think it would still collect location information.

Q What if the person is not doing anything at all with their phone?

A It still could be collecting.

THE COURT: Let me clarify that. Do you mean by not using the app at all that the app is open or closed? It doesn't matter?

THE WITNESS: So the application is not important here once it's enabled. Just the phone being on, not in use, or any specific application being launched or not launched. Once enabled, you are now collecting your location history all the time.

THE COURT: Thank you.

BY MR. PRICE:

Q What about right now? What if somebody in this courtroom had an Android phone? Would it be collecting their location data?

A It very well could be even if they're not using it.

Q How do you know this?
A Again, based on looking at a lot of these records from Location History accounts, not just geofence. Of course, you could get this data just at the account level. The time that it spans when you look at the records, it consistently covers just about every hour of the day, most of the time. So, just looking at it, I would assume somebody's got to sleep at some point or, you know, just not using their device all the time. So it's constantly recording information.
Q And did you review any of those types of records in this case?
A Yeah. So the account that we're talking about here was gathered by law enforcement. So once the particular account was identified, they actually did another request to get the full account. So the location history associated with that account and all the other data that you can normally get through that type of request.

So, in this instance, I looked at that data. So I believe there was a 35-day period of data that was provided in that request.
Q Let's take a look. I'd like to show you Defense Exhibit 8, please.

MS. KOENIG: Your Honor, this exhibit details

very detailed specific location information for an individual, Mr. Chatrie. And so we're going to look at the paper copy of this. This is Defense Exhibit 8, and we would ask that this be put in under seal.

THE COURT: All right. There's no objection to that being under seal; is that right?

MR. DUFFEY: No objection, Judge.

THE COURT: All right. So we'll look at the sealed version, which I don't have a copy of.

THE WITNESS: I don't either.

MS. KOENIG: I hadn't anticipated -- we have a digital copy that had been provided to the Court. I hadn't thought ahead about how to present this since we have broadcasting.

THE COURT: Since we have what?

MS. KOENIG: The broadcasting that is being shown to another courtroom. There's no issue with showing it to everybody in this room if it's up on the screens. I don't know if it's just that I could show it to the witness and the lawyer screens and the Court screen instead of broadcasting it to the other courtroom.

THE COURT: Is there anybody in the other courtroom?

THE CLERK: It doesn't appear that there's

anyone in there.

THE COURT: Can we talk to the CSO and close the courtroom?

MR. DUFFEY: Judge, I guess I'll raise my objection. Why are we talking about search warrant No. 2? I object to relevance if we're going to get into a sealed second search warrant. It's not the subject of the motion today.

MR. PRICE: I'm happy to explain.

Your Honor, the data obtained through that search warrant was Mr. Chatrie's location information over a, let's see, 35-day period. What it allows us to do is to determine how frequently Google was actually collecting Mr. Chatrie's location information. So that point we believe is very relevant, and this goes to show that directly in this case.

THE COURT: I'm going to overrule the objection.

Is the courtroom closed? Do we have an issue with the folks on the phone? Is there anybody on the phone?

THE CLERK: Yes.

MR. PRICE: They won't be able to see it, Your Honor, so it's okay for them to hear the

testimony about it. We just don't want to have the longitude and latitude coordinates being captured or somebody being able to write them down.

THE COURT: Okay.

BY MR. PRICE:

Q All right. So this is Defense Exhibit 8. Can you tell us what we are looking at here?

A Yes. So very similarly to what we have seen when we refer to like the Stage 1, Stage 2 requests. This is account specific location history rather than a group of people's location history. But you'll see very similar items throughout. It will look very similar besides just a few extra pieces of information.

THE COURT: I don't have this document.

MS. KOENIG: Your Honor, it's a very large file. It would have taken hundreds of pages to print off. So we provided it digitally to the Court. It's in the box.com account that we had provided to the Court.

THE COURT: Okay.

BY MR. PRICE:

Q Is this the CSV Google data file that you reviewed?

A Yes.

THE COURT: The what?

MR. PRICE: CSV.

THE COURT: Okay.

MR. PRICE: It's just a type of file, Your Honor. It's a database file.

BY MR. PRICE:

Q This is the file that you reviewed?

A Yes, it's a comma separated value spreadsheet.

MR. PRICE: I'd like to introduce this into evidence, as well, Your Honor.

MR. DUFFEY: Same objection, Judge.

THE COURT: All right. Well, I'm overruling on the same basis.

(Defense Exhibit No. 8 is admitted into evidence.)

BY MR. PRICE:

Q So when you reviewed this file, can you tell us what you found?

A Yes. So, again, this is account specific information for one account rather than a group of accounts. The information contained spans, again, I believe, a 35-day period. And so you'll see that, throughout this document, you'll see dates and times, estimated latitudes and longitudes, those sources that we talked about earlier, Wi-Fi, GPS, as well as those

display radiuses. All of that information is given. This is where the Stage 1 and Stage 2 information actually comes from for each user.

Q So what were the beginning and end dates here, if you recall?

A I don't. From looking at -- the bottom date here is May 1st of 2019.

Q And that's the start date and the end date?

A At the very top it is June 4th of 2019.

Q So it's 35 days?

A I believe so.

Q And could you tell us how many records, how many lines of information are in this file?

A Sure. Can you click on the A column, please? 8,349. And that may include a few rows at the top. I believe there's three rows at the top. So it's 8,346 individual records, I believe. Yes.

Q And were you able to determine about how many records per day that is?

A Yes. So I just took, you know, how many days that was just to try and understand about how many times per day on average that record got entered. I believe it's around 238 times.

Q 228?

A Somewhere around in there. It's an estimate.

Q Did you work out how many times an hour that is?
A Sure. So if you broke that down just by a 24-hour period, that's, I believe, almost 10 records per hour.
Q Or once every how many minutes?
A Once every 10 minutes.
Q Six?
A Sure. It's a lot of data.
Q So 10 times an hour, once every six minutes?
A Roughly. I mean, that's the average. Again, it's not on a specific interval. That's just an average.
Q Were there any times that Google wasn't collecting data? Like, did it only collect data during business hours?
A No. So I looked to try and understand, like, how often per hour, but like the actual hour ranges of when data was collected. And what I did when I looked at that was just try to understand, you know, at, say, 12 a.m. to 12:59 a.m. of every day throughout that period, like, how often it gathered records. And what I noticed was that it was consistently gathering data 24-hours a day. Sometimes some areas had higher rates, some had lower, but regardless, there were no periods of data not being collected. It was a consistent collection of data across the date, if you look at it just on average for that time.

Q There was no hour of the day when Google was not collecting data?
A There could be in certain days. There could have been a day where a particular -- but for the, again, the average of across that time, you could see that it generally always would collect data during hours of the day.
Q So even as you're sitting here, Google is collecting your data?
A Could be, if I had those options turned on.
Q And if you did, how many times would they have collected your data since you've been sitting on the witness stand?
A Quite a few times. I've been here a few hours now.
Q So 20 or so?
A It could be, yeah.
Q Just one last thing. What happens to Location History, the setting, if the user deletes the application that was used to enable it?
A So you're saying in this instance, if Google Assistant was used to opt in to Location History, but then the application is then deleted?
Q Uh-huh.
A So if you delete that, your permissions are still

there. You've enabled that permission on your account even though the application that you used to do so is no longer there. It's not application based. You're activating it for your account.

Q Let me make sure I understand. Even if you delete Google Assistant or even if Mr. Chatrie had deleted Google Assistant, it wouldn't have affected whether Google was getting his location history data?

A No, because other applications are also submitting -- it's still collecting because it's activated for the account, not that specific app. It was just facilitated through an application.

Q So it's a permission for the entire account?

A It is, yes. For that device for that account, yes.

Q Even though it was enabled through Assistant, if you delete Assistant --

A It's still going to collect.

Q It's still collecting?

A Yes.

MR. PRICE: That's all I have, Your Honor. Thank you very much.

THE COURT: We probably should take a break now before cross. It's a natural breaking point, a little earlier than when I normally do it. Do you all

want to break for lunch? It's 12:30.

MR. DUFFEY: Fine with the government, Judge.

MR. PRICE: That's fine with us, Your Honor.

THE COURT: Do you need a full hour? No. Half an hour?

MR. DUFFEY: Yes, ma'am.

MR. PRICE: That will be sufficient. Thank you.

THE COURT: All right. So I'll give a little more than half an hour. I have it as 12:35. We'll turn at 1:15. That will give time for folks to move back and forth. All right?

MR. DUFFEY: That's fine.

THE COURT: Again, sir, you're still under oath. Please don't speak to anybody about your testimony. Don't speak to your witnesses about testimony. And please wait for our CSOs to move you around as you're moving in our hallways. All right?

So we will take a recess, please.

(Luncheon recess at 12:30 until 1:17 p.m.)

THE COURT: All right. I'm going to do our reminders, which is, obviously, that our witness is still under oath. Do we have anybody on the AT&T line?

THE CLERK: Yes.

THE COURT: Anybody who is on our telephone conference, welcome. And I need to remind you that our local rule, Criminal Rule 53, and our standing order prohibits anybody recording, transmitting or broadcasting this hearing.

We have a court reporter here who's making the official record, and that's all we will have of this proceeding.

All right. Thank you. Mr. Duffey.

MR. DUFFEY: All right. Thank you, Judge.

CROSS-EXAMINATION

BY MR. DUFFEY:

Q So, good afternoon, sir.

A Good afternoon.

Q I'm Peter Duffey. I'm with the U.S. Attorney's Office. Nice to meet you.

Let's start -- so we're going to talk about the search warrant first. Phase 1 you've already testified to, but let's just clarify. That's one hour; right? And a fence, 150-meter fence, around the area where we say a crime was committed; right?

A That's correct.

Q And we got back multiple points of data from Google; right?

A In that return, yes.
Q In Phase 1?
A Yes.
Q In fact, the multiple points of data applied to 19 different devices?
A Correct.
Q All right. And we talked about Defense Exhibit 21, which is Mr. McGriff's affidavit, paragraph 13.

MR. DUFFEY: I'm sorry. I should have warned you.

THE COURT: That's okay.

BY MR. DUFFEY:
Q That's where we got the tens of millions of data -- tens of millions number about their location history data; right?
A Correct.
Q And that came from McGriff who works for Google.
A That's right.

THE COURT: Can you repeat the exhibit number, please?

MR. DUFFEY: It's Defense Exhibit 21.

THE COURT: Okay.

MR. DUFFEY: And I'm talking about paragraph 13.

BY MR. DUFFEY:

Q So let me just ask this: You characterize that, or maybe it was Mr. Price, characterized that as a search of tens of millions of people's location history data; right?

A Correct.

Q Mr. McGriff didn't call that a search, did he?

A I don't recall. If we can pull it up.

Q We'll pull it up. But I think you know the answer to this. Let me ask this. This is one database that Google has of location history that they run the parameters that we give them in a search warrant, that is one hour, and longitude and latitude parameters, and ask them to give us location history from those parameters; right?

A Correct.

Q Okay. And it's one database?

THE COURT: I'm sorry. I know the timing of cross is important, but I think -- are we having trouble with accessing the exhibits?

THE CLERK: Laura, it's not coming up on the screen. Is your plug pushed in all the way or whatever they did last time?

MS. KOENIG: I think I got it.

MR. DUFFEY: Thank you, Judge. It's a fairly

minor point.

THE COURT: We're probably going to be using this further. So I want to start off --

BY MR. DUFFEY:

Q So it's paragraph 13 that I was interested in. So maybe if we could just scroll up a little bit to get by that, because I want to see all the words. There we go.

So paragraph 13, they're talking about the majority of Google users worldwide did not have Location History enabled on their account. They concede that it's difficult to come up with an exact number, but one-third of active Google users, tens of millions of Google users worldwide, had Location History enabled on their accounts; right?

A Correct.

Q Now, that's where you get the tens of millions of people's accounts that were searched; right?

A Correct.

Q Nowhere does McGriff refer to that as a search; right?

A No, he's telling you how many people they estimate would use -- that use the Location History service after he discusses that they have to search that database for the people located within the fence.

Q And you would agree with me, we're talking about one database; right?
A The Location History database.
Q Right. That's called Sensorvault, I think?
A I believe that's where they keep it, yes.
Q And when you're talking about searching that, you're really talking about a computer and you're putting in the parameters that you want it to look for; right?
A That's correct. They're using computers to do that work.
Q Also to be clear, the government doesn't have access to the Sensorvault. The government gets the results, that is the 19 devices that Google tells us complied with the parameters that we gave them; right?
A That's right.
Q Okay. So to be clear, when you compared our search here, our geofence search, to a tower dump, the tower dump example we gave you said probably would give 3,000 numbers to the government?
A It's possible.
Q And so we're clear on a tower dump, one, you're getting 3,000 numbers; right?
A Correct.
Q And you're getting phone numbers; right?

A Correct.
Q Phone numbers to people's accounts; right?
A Correct.
Q That is not true in the geofence; right? We're getting reference numbers.
A Correct. You're getting the device ID.
Q Right. But it's a device ID that we, even standing here today after over a year, we can't connect these device ID reference numbers to any individual cell phone numbers; right? At least not through the device number.
A Directly to the phone number? No.
Q Right. And so when you compare 19 devices, and then your Defense Exhibit 3, and that's under seal. So you should have that in front of you; right?
A You said three?
Q Three. That's the return that we got on Phase 1.
A Okay.
Q Actually, I think it also contains Phase 2, but I want to talk to you about Phase 1.
Well, it's not numbered. So if you can click to the very beginning of the actual spreadsheet, and it begins in the upper left-hand corner with the No. No. 1. And that No. 1.
THE COURT: Are you in Exhibit 3?

MR. DUFFEY: Yes, ma'am.

THE COURT: So your face is away from the microphone. So we're not hearing everything.

MR. DUFFEY: Let me move it over here.

BY MR. DUFFEY:

Q So if we can go to the beginning of the spreadsheet that begins with 1 and ends three or four pages later at 210; right?

A Correct.

Q And it's only 19 different devices, but it's actually 209 location plots?

A That's correct.

Q That's what the government got from the search warrant, at least Phase 1; correct?

A Correct, in one.

Q Compared to 3,000 -- possibly 3,000 phone numbers that are identified by their phone numbers in a tower dump; right?

A Correct.

Q Okay. And you testified, I think, on direct that Google calculates to the best that they can that if they are in our 150-meter radius, they're in, and we get coordinates, and if they're out of the 150-meter radius, we don't get anything from them; right?

A Yes. If that latitude and longitude falls

outside, it won't.
Q In, we get it; out, we don't get it?
A Correct.
Q And the latitude, longitude, and that's Column C in -- excuse me -- D and E in this, those are pretty precise. Those are the points that we see you used, I think, in your Mr. Blue, Mr. Green, Mr. Yellow. We've used in some of these where we're pointing; right? So that's the exact point. And then as you move over to G, maps display radius in meters, that's where they say some of these we're very confident on, and they give you a low number in meters; right? And some of these we're not, and they give you a slightly higher number; right?
A That's correct.
Q So that's like their margin of error, say, in a, I don't know, a political poll, they give you a margin of error. This is like Google's margin of error. They're telling you how confident they are, and how close this phone is likely to be to this -- to those longitude and latitude marks?
A That's correct.
Q And some they're pretty confident in, and some they tell you we're not so confident in; right?
A Based on radius, right.

THE COURT: Based on what?

THE WITNESS: The radius, how big or small it is.

BY MR. DUFFEY:

Q If we could go to Government's Exhibit 1, page 20. And that's with the big blue circle. On direct, you talk a lot about this because this -- and you're accurate. This one big blue circle included businesses, and streets, and apartments, and all kinds of things; right?

A Correct.

Q All right. And I think you testified that the margin of error, so to speak, the map display radius on that was 384 meters.

A Somewhere around there, yes.

Q That's pretty high?

A Yes.

Q In fact, if I can get you to look through the Stage 1 returns, so let's start with the page at the very beginning of the returns. In the upper left-hand corner, that's a one, and it goes down to line 33; right? Are you with me?

A Yes.

Q Looking at map display radius, do you see any numbers in that that are even close to 384?

A No.
Q In fact, I think it's lines two, three, four, and five, maybe the first six or seven are over 50, but none are more -- there's two that are 100 even, and then the rest are less than 50 meters; right?
A That's fair, yes.
Q Is that right?
A Yeah, it is.
Q Okay. Second page, likewise. That's line 34 through 66. There's not a single map radius that's over 50 in that; right?
A Correct.
THE COURT: Wait. Where are you?
MR. DUFFEY: Going to the next page.
Q And that has line 67 through 99. I think there's only two, which is line 83 and 86, are slightly over 50. The rest of the display radiuses are under 50; right?
THE COURT: Can you remind me which exhibit we are?
MR. DUFFEY: We are Exhibit 3. And then we're at the third page of the spreadsheet. And that has lines 67 through 99.
THE COURT: Got it.
BY MR. DUFFEY:

Q So, I'm asking you, with the exception of line 83 and 86, which are slightly over 50, the rest of those map radius numbers are all under 50 meters; right?
A Correct.
Q We go to the next one, that's line No. 100 to 132, the entire sheet's well under 50; right?
A They're under 50, yes.
Q Not a single one's over 50?
A It's not --
Q Much least 384?
A That's right.
Q Similarly, line 133 to 166, that page, I think there's two. One's 104 and one's 122. Well, let me be precise. Line 137, slightly over 100. And line 150, a little over 100. The rest significantly lower. In fact, some of them are down to 3 meters; right?
A Correct.
Q In your training and experience, being down to 3 meters is probably a GPS point; right?
A It is. A reference is GPS for those points.
Q All right. Very similarly, on the next page, line 166 to line 198, lots of GPS points. Nothing -- excuse me. One over 50. Line 186 shows 73. The rest well under 50; right?
A Correct.

Q So, finally, the last page.

MR. DUFFEY: I'm getting to it, Judge.

Q 199 to 210, the very end of Phase 1. The second to the last one there, line 209, that's the three -- excuse me, 387, I think it is. That's the blue circle; right?

A The largest one, yes.

Q Right. Now, if you look right above that also at line 208, that's the same reference number; right?

A Correct.

Q So that's the same device; right?

A Correct.

Q And only about 30 seconds earlier, but their radius -- map display radius on that is 84?

A Correct.

Q So they have the same device on here. It has a map radius of only 84, but the next one for some reason goes to 387.

A Correct.

Q Do you know why it jumped to 387?

A I don't.

Q Do you have any idea?

A I don't.

Q Okay. But you would agree with me, if we take away that one anomaly, which is the only one in this

entire Phase 1 that's even close to 387, if you remove that one anomaly, what we're left with is a fairly concise circle. Granted, some of them are slightly outside the geofence radius. But it's fair to say this one, the one big blue circle, is pretty much an anomaly here; right?

A Again, it's larger than the others, and it's the only one.

Q Well, it's a lot larger than the others; right?

A Yes.

Q Okay. And, in fact, the coordinates just 30 seconds earlier on that same device was only 84; right?

A Correct.

Q Okay. So, now, we've got -- as I said, Phase 1 was 19. I'm calling it anonymous numbers. I know you don't agree with that, but these were 19 devices. So let's talk a little bit about the anonymity of these. The reference numbers here, and those are all those reference numbers in Column A from the Phase 1 thing; right? You've been looking at this for over a year; right?

A Correct.

Q Is there some secret code to those reference numbers that you've cracked that can tell you what the

cell number is that's associated with those reference numbers?

A No.

Q And so to your knowledge, I mean, when we're talking about anonymity, those reference numbers are anonymous as far as identifying any particular phone number; right?

A Correct. They don't associate to a phone number.

Q So we can take out the reference number. That's not what you're talking about when you say the returns aren't anonymous; right?

A Correct.

Q Okay. Now, as we talked about the map radius, the location is not precise, and Google gives you different margins of error; right?

A Correct.

Q Some very, very small and some larger. But every single one of these plots that we got back, Google reasonably believes, at least in their mind, that every single one of these by longitude and latitude should be plotted within our 150-meter radius; right?

A That's how they returned it, right.

Q And if they found a longitude and latitude outside of our radius, we don't get it; right?

A Right.

Q So there's no search as far as the government is concerned. We don't get any information on that device; right? Is that right?
A If the point falls outside of the geofence, you don't get it.
Q Okay. They're not guessing at this. They're not -- it's not their discretion. They have a set way of doing this; right?
A They certainly do.
Q And they calculated longitude and latitude; right?
A Yes.
Q And they comply with the search warrant and the parameters that we give them; right?
A Correct.
Q So at this point Phase 1, in your mind, is anonymous; right?
A Sure. You only know who's inside -- you only know the numbers for the people inside the circle.
Q And you have these anonymous reference numbers; right?
A Yes.
Q They don't give you any clue; right?
A No, they just associate --
Q So Phase 1 is anonymous just like everyone says; right?

A Sure.
Q Okay. Phase 2 is where you begin to diverge a little bit; right?
A Correct.
Q Okay. So let's talk about that. So -- well, first, let me ask you, you said government -- the government asked in Phase 2 for all 19; right?
A Correct.
Q From Phase 1. And I think you said, but I'm not sure, was it your testimony that then Google decided to give us only nine?
A No.
Q What did you say?
A It was that 19 were requested and that Google asked for them to be -- for that number to be reduced.
Q Right. Well, I think they just didn't respond. But --

MS. KOENIG: Judge, objection that Mr. Duffey is, I think, testifying about that point instead of the witness.

MR. DUFFEY: Well, it was a question.

THE COURT: The question is, what you think? How does he know what you think? Just rephrase it.

MR. DUFFEY: All right.

BY MR. DUFFEY:

Q The point is, is that Google didn't respond to the initial request. I mean, you reviewed the emails; right?
A Yes.
Q Google didn't respond to the government's first request that we get all 19 back; right?
A I think that's right, yes.
Q And, in fact, a couple of times when we asked, Google just didn't respond?
A Correct.
Q And it's also true, then, that -- and this is Detective Hylton's email, I think. He added in, in the alternative, here's our nine; right?
A Correct.
Q And so those nine numbers weren't chosen by Google. They were chosen by Detective Hylton?
A Correct.
Q Okay. Just so we're clear on that. And all nine -- did you do the plot, all nine videos, too? Did you plot all nine of those?
A Yes.
Q And, in fact, all nine of those, if you recall, all the radiuses, with, I think, the exception of one, all fell -- not only the point, but the radiuses, too, the map display radiuses, all fell within the

150-meter circle. Does that sound right?
A I think that's correct.
Q Now, so let's talk about that. So then it's your contention, then, though, that once we -- in Phase 2, we drop the fence. We add a half hour to each end. That's what we did. That's what the government asked for in the search warrant; right?
A Correct.
Q And so now we're talking about two hours on one particular day with no geographical restriction and just on these nine phones; right?
A Correct.
Q So, basically, we already know some of this because we've had them in Phase 1; right? But now we're going outside the circle; right?
A Correct.
Q So, in some of these, your contention is it's not really anonymous because they go -- I think you really center on the fact that they travel -- they appear to travel to a single family residence; right?
A That's part of it, yes.
Q Well, we'll talk about that, then. So, when they go to the residence, would you dispute that not a single one of these in Phase 2 of these nine phones stay at any single family residence more than an hour?

A Do they stay there for more than an hour?
Q Right.
A We've only got two hours of data. So none stayed for more -- no, none stayed for an hour.
Q Less than an hour?
A Sure.
Q Okay. All nine phones, when you mapped them out, none of them stayed at the -- I realize you're tracking them. They're going down roads. At some point, they're all going into the circle; right? At least that's what we say; right?
A Correct.
Q And then some of them go back. But none of them stay at any single family residence for more than an hour; right?
A Correct.
Q And many of them don't even stay very long at all; right?
A Correct.
Q Okay. Now, you would agree with me that -- I mean, how old are you?
A Thirty-three now.
Q All right. You've been to people's homes and stayed more than an hour; right?
A Sure.

Q You didn't live there; right?
A That's correct.
Q In fact, people get guests at their homes all the time; right?
A That's right.
Q So you're not saying, as an expert, because you can track a cell phone to at or near a residence, that that means they have to live there?
A That's right. That doesn't mean they have to live there, you're right.
Q I understand you say it's possible, and I would agree with you it's possible. Anything's possible. But that doesn't mean that they live there; right?
A That's correct.
Q And I think when we're talking about -- I notice when you plotted on your three plot -- let me get the number. Defense Exhibit 5. We don't have to play it, but in that you plot specific points, and you show them hitting at or near a single family residence. And that's for Mr. Green, and Mr. Yellow, and Mr. Blue; right?
A Correct.
Q So, I notice we don't have the map display radius around those points; right?
A That's correct.

Q Isn't it fair to say that many of those, if you put up the map display radiuses, would probably include the house next to it?
A That's right.
Q In fact, I think you said that on direct.
A I did.
Q In fact, it might include a third house; right?
A It could include more than one, yes.
Q Okay. So, now, you don't know whether they're a guess or the actual person who lives there; right? And for most of these, if not all of these, you're going to have to look, if you want to figure out their identity, now you're looking at two, maybe three houses; right?
A Correct.
Q And you would agree with me that if, in fact, the holder of that phone was a guest, then doing the things that you talked about doing, the open source thing and looking at tax records or deeds or I'm not sure what, you weren't real specific on what you were looking at, but looking at those kinds of things, like deeds, tax records, open source data, for that house, if they were a guest, then you're not going to get that; right?
A Right. You're going to see the person they're

associated with.
Q Right. And nobody on their tax record or maybe you get, I don't know, their power bill, no one says here's Peter Duffey's power bill, and, by the way, here's 10 of his closest friends; right? You're not going to get that off the power bill; right?
A Correct.
Q So I think you would agree with me that if, in fact, these people were a guest in the home that you're looking at, then you're not going to be able to find their name from any of this open source data that we talked about; right?
A Probably not.
Q So now we're talking about you're having to limit this, and you're having to assume, I guess, or look for them actually living in the house before you even have really a prayer of figuring out their identity; right?
A For associating with the house, then, yes, you would need something.
Q Well, the phone is the only thing that associates it to the house; right?
A Correct.
Q And so what we're talking about is identifying the person holding the phone; right?

A Correct.
Q And when I say "identify," and you tell me if you agree with me, when we're talking about identifying a human being, you're talking about their name; right?
A Sure.
Q Okay. So all of these, I guess, you could go to the courthouse, if you had an address, and look at the deed; right? You could get other open source data, figure out who paid the taxes on the house; right?
A Yes.
Q That would give you the owner?
A Correct.
Q But you'd agree with me, if the owner was leasing the house, then you're back in the dark again because now there's lessees in the house, and you don't know who they are; right?
A That's right.
Q And you won't get that from any of this open source data?
A Right.
Q And, of course, there's Facebook; right? I think you looked on Facebook.
A Correct.
Q Other tax records. All of this, you would agree with me, requires fairly significant investigative

work on your part; right?
A Yeah, you have to look into the data.
Q None of it come from Google; right?
A Correct.
Q And none of it certainly came from Google pursuant to this search warrant; right?
A Correct.
Q Okay. So let me ask you this: Ultimately, if you were to get, say, a person's -- even if you were able to figure out what their phone number was living in a house, and then you had one of our phones from Phase 2 going to that house, you'd still have to be able to match up their phone number with this anonymous reference number from our Phase 2 data; right?
A Correct.
Q Because there's nothing in the reference number that we got pursuant to this warrant that tells you what their phone number is, at least until you get to Phase 3; right?
A Correct.
Q So even then, in order to match up that phone to that person, you're going to have to probably have a friendly prosecutor, and you're probably going to have to do court process; right?
A Yes.

Q You're going to have to get a search warrant; right?
A Yes.
Q At least grand jury subpoenas to figure out who the subscriber to the phone was?
A Yes.
Q Maybe. And even -- and you were in law enforcement for eight and a half years, so I think you're going to know the answer to this. Criminals often use other people's names on their cell phones; right?
A People in general do that, yes.
Q Okay. And especially, say, drug dealers; right?
A They can, yes, or false names more often than not.
Q They do it all the time; right?
A Yes.
Q Or they use a girlfriend's name; right?
A Correct.
Q Because they don't want their name associated with the phone.
A Right.
Q So in your, I guess, scenario of saying you can maybe uncover the identity of these people, even if you got a person's cell phone at this house and got the subscriber information and figured out their name,

that still doesn't get you there; right? Because you're not sure, one, whether or not they were the ones holding the phone on May 20th at 5 p.m., or whatever the time is, of 2019; right?

A Correct.

Q The time of this search warrant.

A Right.

Q All right. So when -- I guess maybe it's a question of semantics, but I just want to ask you, so it's your expert opinion that the information that we got from Google in Phase 2 is not anonymous?

A It's not that it's identifying in terms of names, but, yes, it can lead you to know who that person is based on being able to track where they have been.

Q Okay. In two hours of one day; right?

A Correct.

Q You think you can figure out who these people are?

A Sure.

Q All right. Have you figured out who anyone is?

A I haven't, no.

Q Well, you've had over a year. You haven't figured out the identity of anyone in Phase 2?

A I wasn't actually here to investigate who the people were. I was trying to determine if it would be possible to do so.

Q Okay. But you haven't done it yet?
A No, I have not.
Q Okay. So when you say it's not anonymous, it's because it could lead you, with extra work, extra investigative activity, maybe lead you to possibly a group of likely suspects; right?
A Correct.
Q And in your mind, that means that's not anonymous?
A Right.
Q All right. So let's talk about, if we could, your supplemental report. And that's Defense Exhibit 7; Right?

MR. DUFFEY: Could we get that up? Do you mind?

MS. KOENIG: Sure.

BY MR. DUFFEY:
Q So you would agree with me, looking at your report, right off the bat, you state, and I think everyone appreciates your candor, that you can't replicate the opt-in process that the defendant would have seen. That's on page 1 of your report.
A That's right.
Q So you can't be sure exactly which of these screens that he saw, if any, from your report; right?
A Can't be 100 percent certain.

Q Sure.
A Right.
Q And so the Quartz article, which is Defense Exhibit 48, and we don't have to get that up, but that's what it is, you show the screenshot in your report, Defense Exhibit 7, as Figure 1; right?
A Correct.
Q And I think you said this, but let's make it clear, this article was published January 24th of 2018; right?
A Right.
Q And I think we've established that Location History on our phone -- I say "our phone" -- the target cell phone here, Mr. Chatrie's phone, was enabled on July 9th of 2018; right?
A Right.
Q So you would agree with me that the Quartz article showing various screenshots was published seven or eight months prior to the enabling on Mr. Chatrie's phone; right?
A Correct.
Q Okay. And we'll get to the Norwegian test, but that shows a different -- that's from July, and that shows a different screenshot; right?
A The Norwegian?

Q Yes.
A Yes, correct.
Q So either Quartz is just wrong or something changed in between January and July; right?
A Correct, the language changed.
Q Okay. So when we look at Figure 1, and this is Figure 1 on Government's 7, this is the Quartz screenshot; right?
THE COURT: Just to be clear, it's Defense 7.
MR. DUFFEY: Oh, I'm sorry. Defense Exhibit 7.
BY MR. DUFFEY:
Q Figure 1, this is the Quartz screenshot; right?
A Correct.
Q And you would agree with me, this is not entirely accurate because it cuts off "No, thanks" or "Yes, I'm in" at the bottom of the screenshot; right?
A Yeah, it has to be scrolled down to get to those.
Q Okay. So we can assume that at the bottom there is a "No, thanks" or "Yes, I'm in"; right?
A Correct.
Q Okay. And can you preclude the possibility that if you click "No, thanks," that there's a second opt-in page that follows up this to say, like, are you sure, or this is what happens if you do this?

A I'm not sure if there is.
Q You don't know?
A No, I don't.
Q In fact, the Quartz article, it wasn't really the point of the Quartz article to document the opt-in process; right?
A Right.
Q They had a different subject; right?
A Correct.
Q It wasn't about whether or not this is truly an opt-in process; right?
A No. I used the screenshot because it showed one of the permission screens.
Q Oh, I'm not attacking you. I'm just pointing out the point of the article wasn't about opt-in. It just happened to have screenshots in it; right?
A Correct.
Q Okay. The second source you went to, the Oracle report -- for the record, that's Defense Exhibit 11. So if we go to page 2 of your report, Exhibit 7, so Figure 3, in this screenshot that you document -- excuse me, Figure 2. This is page 2.

MS. KOENIG: It's page 2 of Exhibit 7.

MR. DUFFEY: All right.

BY MR. DUFFEY:

Q This doesn't document at all when this screenshot would have been taken; right? Or does it? You tell me.
A I think in another portion they do reference when -- I know they were 2018. I'm trying to recall. I think it was -- I think it was actually closer to the time frame of Quartz, if I'm --
Q Before July 2018?
A I do believe it was before July.
Q But looking at this, you're not sure because it doesn't document it in your report?
A Not right here, no.
Q Okay. And, again, much like the Quartz figure, the Quartz screenshot, this does not document if there's any further opt-in or out-out process after clicking either "No, thanks" or "Yes, I'm in"?
A It does not.
Q It doesn't tell you what happens next?
A No, there's no screenshots for that.
Q Okay. Now, then we go to the Norwegian report, and the Norwegian report itself was Defense 27, but this is on page 3; right? And the difference here, I take it, is that you have to opt-in, I think you testified. It now has three things in the opt-in list, I guess you would call it, that has Location

History. And this is Figure 3, "Location History, Device information, Voice & Audio Activity"; right? And those all three are on the list; right.

A Yes, they were on the others, as well.

Q Then you also show the expanded view of Location History. That, I guess, is that you clicked on the down arrow, and that gives you an explanation of what Location History is; right?

A That's what they did, yes.

Q Okay. And that says "Location History saves where you go with your devices"; right?

A Yes.

Q To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, such as Google Maps or Search. That's on Figure 3; right?

A Yes.

Q You're not contesting that a normal consumer reading that could not figure out that Google is saving their location history, are you?

A No.

Q Okay. So it's clear, pretty much to anyone who can read, that they're telling you Google is going to save where you go; right?

A Correct.
Q It also says "If you use the device without an internet connection, your data may be saved to your account once you return online"; right?
A Correct.
Q I think that goes to your point that once you enable Location History, it's tracking your phone all the time; right?
A Right.
Q Okay. It also says, I think, that this data may be saved and used in any Google service where you were signed in to give you more personalized experiences; right?
A Yes.
Q And it tells you, you can see your data, you can delete it, and you can change your settings at account.google.com; right?
A Correct.
Q That's the same language that Mr. McGriff has in his affidavit; right?
A Correct.
Q Okay. So there's nothing shady about that; right? About McGriff's affidavit, at least to that point; right?
A No.

Q Same language. All right. And then at the bottom, again, there's "No, thanks" or there's "Turn on"; right?
A Correct.
Q Do you think there's any ambiguity there that you are turning on Location History?
A No, it's specifically asking for those three permissions.
Q All right. And, essentially, and I think this is Defense Exhibit 23, is McGriff's affidavit, the difference really with McGriff's affidavit is that -- in his affidavit and his screenshot, Location History stands alone; right?
A Correct.
Q That's really the only difference; right?
A Correct.
Q He doesn't define Location History any differently; right?
A No.
Q Okay. And there's still a "No, thanks" or "Turn on" at the end of it?
A Correct.
Q Right. So is there any doubt also that consumers are told -- and this is true, that they can always delete Location History any time they want; right?

A They can, yes.
Q So I know Mr. Price asked you about turning off or, I guess, deleting Google services or Google Assistant doesn't turn off Location History?
A Right, the application.
Q Right. My question is, though, regardless of that, any time a consumer wants, they can go on their phone and they can say stop taking my -- stop saving my location history; right?
A Correct.
Q And then Google will stop doing it?
A Correct.
Q In fact, they can delete it, and then Google won't have it in the Sensorvault anymore; right?
A Correct.
Q And if Google doesn't have it in the Sensorvault, the government's not getting it even with a search warrant; right?
A The way I understand it, yes.
Q Because it's just not there.
A Right.
Q So that can come either because the person never turns on Location History; right?
A I'm sorry?
Q That can happen -- the government can, I guess,

get thwarted on the search warrant by Google where Google says "We don't have any location history." That can happen for two reasons. One is the person, the holder of the phone, can have never turned on Location History; right?

A Right.

Q Or they can at any time go back on and delete it?

A Correct.

Q Any time before the search warrant comes; right?

A Correct.

Q In which case, in both cases, Google, in response to a government search warrant, would say, Sorry, we don't have anything; right?

A I would think so, yes.

Q Okay. And I think you've said this, again, but let's make it clear. There is no way that Google saves this data without the customer in some form or fashion clicking either "Yes, I'm in" or "Turn on" and Location History is at least one of the items up above that choice; right?

A Right.

Q A customer has to agree to Location History or Google is not saving their location data; correct?

A Yes, their location history. It doesn't have that.

Q From Mr. McGriff's affidavit, do you have any reason to doubt his one-third of Google users worldwide have Location History enabled? That means two-thirds do not; right?
A Yeah, there's no way for me to know.
Q Do you have any reason to doubt that?
A No.
Q I mean, you talked about the tens of millions number on direct; right? You got that from the one-third of Google users worldwide having Location History enabled; right?
A Correct.
Q That means three times that number of Google users don't have Location History enabled; right?
A That's right.
Q Which means they're not -- Google has none of their location data; right?
A They don't have location history.
Q Location history.
A Yes.
Q We'll get to that.
So, it's fair to say that tens of millions of Google users have somehow figured out how to use their phones without Location History enabled; right?
A Right.

Q There's millions of people using their phones without Location History enabled?
A Right.
Q You're not saying in your opinion these people, I don't know, are just stupid because they don't know how to turn it on?
A I'm not saying anything about those people.
Q Does that seem reasonable to you that tens of millions of people would be using a phone without Location History when they really wanted Location History on?
A I don't know why you would make the choice one way or another. That's completely up to the user.
Q All right. Okay. Well, let me ask you this: Location Services is clearly not the same thing as Location History; right?
A Right.
Q So Location Services, enabling that, that's what really gets you, I guess, according to Google, kind of the fun stuff of the phone; right? That allows the phone to know where it is at all times; right?
A Right.
Q Realtime?
A Right.
Q And so if you wanted to -- you have Location

Services enabled, you can turn on Google Maps and say, Take me to the nearest Chick-fil-A, and it will tell you right then, Go down the road, take a right, and it will direct you there; right?

A Right.

Q Because it's tracking you realtime because you have Location Services enabled; right?

A Right.

Q And you have Google Maps enabled and all the other things; right?

A Right.

Q But that is not the same thing as Location History; right?

A No.

Q Because if you have Location Services enabled, you can do all the fun stuff that I call it, but without Location History enabled, Google's not saving any of that; right?

A Not that I'm aware of, no.

Q It doesn't go into the vault; right?

A I'm not sure. I don't know for sure. That would be Google, but --

Q Well, I'm asking you, in your expert experience, if you don't have Location History enabled, Google's not saving the data; right?

A It's not saving Location History. I don't know if they're still saving some location information is all I'm saying.

Q Well, do you think they're saving your Location Services data when you've told them not to enable Location History?

A So, look -- yeah, Location History is you creating that data that's being stored to you. There's still advertising data and things being collected. I just was trying to say, as far as Location History goes, you can have Location Services running and either have Location History either running or not. Two different things away from whether or not they still collect some location data in other ways. But as far as Location History goes --

Q They do not?

A Right.

Q So if Google tells you that the only thing the government gets from a search warrant is Location History, do you have any reason to doubt that?

A No.

Q And, therefore, I'm asking you if Location History is not enabled, the government's not getting any location data out of Google; right?

A Correct.

Q We've talked real quick about our second search warrant, and that's Defense Exhibit 8. And that had a whole bunch of plots; right?
A Yes.
Q That's the second government's search warrant that focused just on Mr. Chatrie's account; right?
A Correct.
Q It had a whole bunch because we covered, I think, a little over 30 days of him traveling around; right?
A Correct.
Q But you're aware that that came after he was ID'd as the likely suspect of this crime; right?
A I understand that.
Q I mean, Google didn't pick him; right? We picked him; right?
A Correct.
Q And as I think I just said, this was a search warrant; right?
A Right.
Q It was issued to Google; right?
A Correct.
Q Signed by a judge or a magistrate; right?
A Correct.
Q Okay. And I think you were asked, but if we could go back to Government's 1, page 24. This is, in fact,

the device ID ending in 5659; right?
A Correct.
Q This is Mr. Chatrie's phone?
A Correct.
Q That's what we said. You would agree with me that this is pretty precise information about Mr. Chatrie's phone; right?
A Yes, sir.
Q In fact, all the red dots on the corner there are GPS marks; right?
A That's correct.
Q And all of the map radiuses are completely within the 150-meter geofence with the exception of one; right?
A Correct.
Q And it's multiple hits both around that large church and also around the bank; right?
A Right.
Q In your law enforcement experience, do you question why the government would have gone after a second search warrant on this phone?
A No.
MR. DUFFEY: Judge, if I could just have one second, I think I'm about done.
All right, Judge. Thank you. I think I'm

done.

THE COURT: I do have one question.

Sir, do you know how towers store information? Do they store it by tower? So if you're doing a tower dump, what are you downloading?

THE WITNESS: So the carriers will look for how they store it. I don't know if they store it, necessarily, tower per tower, but when they do that search, they are searching based on the tower location. So they will query for, you know, in the tower dump instance, a period of time for a specific tower that the location referenced. It's searched based on usage of the tower.

THE COURT: So you don't know if the download comes from just the tower or from a bigger database?

THE WITNESS: Likely going to come from a larger database. I doubt that the tower location is holding all of the records.

THE COURT: All right.

MR. DUFFEY: May I ask two follow-ups to that?

THE COURT: Of course.

BY MR. DUFFEY:

Q So, first, to be clear, when you're talking tower dump, you're getting that information not from Google,

you're getting that from a cell phone provider; right?
A Correct.
Q So that's Verizon or AT&T or T-Mobile or some of those people?
A Correct.
Q And I think the Judge's question about what database it comes from, tower dumps, we give them or law enforcement gives them an address; right? And they say, Here are the likely towers that if that person was near that location, here are the likely towers that they were hitting off of; right?
A Correct.
Q That a phone would have been connecting to; right?
A Yes.
Q And then they get -- I guess, to clarify, the data is not stored at the tower, but the data is stored and saved, I guess, through each tower; right? Meaning once Verizon figures out, Okay, there's two towers that are at issue here, they go back. They're searching their database just for those two towers; right?
A Right.
Q To figure out which phones likely were hitting off of those towers; right?
A Correct.

Q Okay. And, again, then they give up actual phone numbers, not anonymous reference numbers; right?
A That's right.
Q Okay.
MR. DUFFEY: That's all I have, Judge.
THE COURT: Okay. Thank you.
MS. KOENIG: Your Honor, I'm going to try to do this myself up here at the podium, but I'll need to have the screen switched to the podium monitor, please. Perfect.

REDIRECT EXAMINATION

BY MS. KOENIG:
Q All right, Mr. McInvaille. Before I lose track of my last thought, in terms of the tower dump, so when -- is it -- how does a phone -- when we have a tower dump, what is the number doing? Like, the phone that is received in the tower dump, what does it mean that that phone has done with that tower?
A Generally, it's because a call or a text -- in most cases, it's because a call or a text has occurred.
Q Like, did it connect -- did that particular device connect with that tower?
A Yes.
Q And so when the company is searching for all the

devices that connected with that tower, is it just looking for the phones that connected with that tower?

A Yes, it's the ones that they actually have records for. So, again, kind of in that scenario of earlier when you asked or when it was asked if a phone is just sitting idle, while it will communicate or at least interact with the network, that's not information that's generally, it can be in some cases, recorded.

Most of what you see in the tower dump is due to calls or texts. There are other instances, but that's generally what's being requested.

Q If I'm a judge, and I'm issuing a warrant for, like, a tower dump of Tower A, does that require the phone company to look through the data for the phones that connected to Tower B?

A I don't think so. I would think they would be able to narrow it down just by the tower that they are actually looking for.

Q Because it's specific to, like, a -- they record the data as to which tower it connected with; right?

A Right.

Q Okay. Let's go way back to the Google account itself. And so we've talked about a Google account that's at issue in this case. Is the Google account in this case a Gmail account?

A Right, it is.
Q So when we say "Google account," we're meaning that Mr. Chatrie had a Gmail email address?
A Yes. You have to create one for an account.
Q Okay. What type of phone did Mr. Chatrie have?
A It was a Samsung S9.
Q Is that an Android phone?
A It is.
Q Who makes Android?
A The Android operating system is a Google product.
Q Okay. When we go back to Mr. Duffey's questions about the search that's run in the Stage 1 returns, do we know how Google runs the return?
A Other than looking inside of the Location History database and drawing, you know, actually using the latitude and longitude to figure out where at -- you know, if this data would actually fall within there. That's all I really know about how they conduct that search through that database with the latitude and longitude.
Q So let's go back to that latitude and longitude point, and let's talk about it in context of Wi-Fi and GPS. When we looked at Defense Exhibit 3, what are the two types of sources of data, the location data, that are in that Stage 1 return?

A And you're referring to the Wi-Fi and GPS portion?
Q Yes.
A Yes, those are two of the sources that are in there.
Q The GPS and Wi-Fi?
A Yes.
Q So what is GPS? I know you said it was Global Positioning System, but what does that mean?
A So that's using satellites to locate a GPS-enabled device.
Q So I've got my phone in the courtroom. If I'm connecting to a GPS satellite, how does that work?
A So, you don't really connect to it. The satellites are broadcasting information down that can be used. So GPS, you don't have the issues of loading up the GPS system. It's because you're just receiving the information. Your device is resolving where it is based on the information it's receiving.
Q And that's very accurate information?
A It can be.
Q And then with Wi-Fi, how do we generate Wi-Fi location data if a phone connects to a router?
A So, very basically, as far as how Google does it, it is based on generally knowing where the access point is, because they don't know the exact place

within, say, your home that your access point is, but they're able to figure out that, hey, this access point is generally here at Laura's house.

Based on signal strengths, they can measure to and from that device. Then you can, with a few of those, resolve if I know where points A, B, and C are, and the phone is getting signals from A, B, and C based on signal strength, and probably some other information that they put along with that, they're able to resolve a location.

Q So I want to make sure because this is, I think, a compact issue. Let me make sure I understand each point.

So, somehow Google has determined where all these Wi-Fi routers are?

A We, or Google users, share that information.

Q How do we do that?

A Your phone -- one of the things that you'll set up in the initial setup of a device is whether or not you want to share that type of information with Google. I don't recall the specific wording of it, but there is a place in here, Would you like to share that type of information? So being able to, say, share with Google, this is a -- you don't specifically tell them this, but your phone will tell it, like, hey, I'm

here. And this is also what I see at the time, so that it can be used later to make those type of requests.

Q And so when we see in Defense Exhibit 3 in the column that is regarding the sources, when we see a Wi-Fi connection, does it mean that that phone has actually connected to that router?

A No, it's not like going somewhere to, like, your friend's house and connecting to the Wi-Fi. It just simply sees the identifiers for that access point that it's broadcasting. A connection between those doesn't have to be, like, user name/password kind of connection.

Q So if I'm at my house and I have a Wi-Fi router, and I have shared somehow this information with Google that I have a Wi-Fi router, do they keep that information?

A Yes. You don't have to share it. It could be your neighbors that your neighbor's device or something picked this up and shared it. It's a community effort, pretty much, through Google.

Q And so if you happen to be driving past my house, can your phone see my Wi-Fi router?

A It's possible, depending on how far away it is, things like that. But, yes, in general, your phone

would -- you know, say it's in close proximity to the road, you could see yours and your neighbor's, as well.

Q So if you are -- if in the points of data that list out Wi-Fi, it doesn't mean that the person was at the -- like, in the building or in any way associated with the router from the place that the Wi-Fi is indicating there's a longitude and latitude?

A Right. It's not a user name/password interaction. This is just that it sees the identifiers for that specific point.

Q What do you know about the ranges of Wi-Fi routers?

A Generally, probably looking at 150 feet or so for a normal router. I'm sure you could -- you know, different sets could be bigger or smaller, but that's kind of generally what people look at.

Q So when Google is estimating the longitude and latitude that's listed in Columns D and E of Defense Exhibit 3, how are they estimating that longitude and latitude?

A Again, with Wi-Fi, it's because they're using those -- the kind of mostly known location of access points, signal strength values, to resolve a location.

Q So if a Wi-Fi point, the longitude and latitude is

based on where Google thinks the Wi-Fi router itself is?

A That's a piece of it, yes.

Q And so when you're looking at the Wi-Fi data point that's plotted, the longitude and latitude, we're not talking -- or are we talking about the longitude and latitude that Google thinks the device was at or where the connection to the Wi-Fi router is?

A That's where it thinks the device was at that given time.

Q But within this larger radius?

A Correct.

Q So the phone or the device could be anywhere within that blue circle?

A Correct.

Q Okay. I want to turn to Defense Exhibit 3. And if you'll look -- we've been talking a lot about the Stage 1 returns, which I think begin at page 6 and maybe end around page 12, and I want you to look at the Stage 2 returns.

A Is that in the same --

Q In the same exhibit. The Stage 2 portion of Exhibit 3, which is the second spreadsheet.

A Okay.

Q Does that portion of Exhibit 3, the Stage 2 data

returns, does that also have a maps display radius?
A Yes, all of the Location History data does.
Q Can you look through those map display radiuses and tell us some of the larger numbers that you see?
A On the first page, the largest is 179. The smallest, I believe, is 16, it looks like.
Q Let's go to the next page.
A This page, the largest is 413, it looks like. That's on line 42.
Q Let's go to the third page.
A Line, it looks like, 75 is 164 meters.
Q Then let's go to the next page.
A 100 meters is line 104.
Q Okay. The next page.
A Line 157 is 1,797.
Q And let's go to the next page after that.
A Line 170 is 64.
Q What's the next page after that?
A 156 meters, line 231.
Q Next page after that.
A Looks like 55, which is line 264, 55 meters.
Q Can you go to the next page?
A 210. It is line 292.
Q Let's go to the next page after that.
A Line 322 is 1,573.

Q Let's just have you kind of more quickly flip through and tell us if you see any other large numbers that are over a thousand.
A It's the page that begins on the Column 397 or Row 397 through 429. Row 420 is 1,026. The final page begins with Row 661, ends in 681. The Row 681 has 1,838 meters.
Q Okay. So is it fair to say that the map display radius varies depending on the longitude and latitude point, the individual data point?
A Each point has their own display radius.
Q Had the geofence swept in one of these data points that had a map display radius of over a thousand feet, the effective radius of the geofence would have been multiple thousands of feet just in the radius, in the diameter?
A If you look at it as if the -- if that point had fallen within the fence and that circle extended, and then if the phone could be anywhere within that circle, then I guess you could look at it that way.
Q So is there any way for a judge or law enforcement to know ahead of time what the effective radius of the geofence is going to be?
A I guess knowing what I know is that the only thing that you can, as far as that search goes, is knowing

that the estimated latitude and longitude would have to fall within the circle for it to be captured.

Q But the effective radius could end up being thousands of feet or meters larger than that; right?

A In that scenario, I guess, yes.

Q I want to talk about the device ID that's listed in Column A of Defense Exhibit 3. The government asked you a number of questions about whether that's tied to a phone number, and you've indicated that you don't have any information that it is. Is that right?

A Correct.

Q Have you reviewed Ms. Rodriguez's declaration, which is Defense Exhibit 24?

A Yes.

Q By Ms. Rodriguez, I mean Sarah Rodriguez from Google.

A I have.

Q And in reviewing that, do you have any indication that the device ID remains the same from one geofence search to another?

A Say that again.

Q In reviewing Ms. Rodriguez's affidavit, does it indicate to you whether the device ID, that number in Column A, remains the same for each device from geofence search to geofence search?

A The way it's described, it appears that the kind of global identifier that would face out through the accounts is stripped, but that that number that you see within these requests is an identifier that stays with that particular device, but only within the Location History database. It does not reach outside of that database.

Q So if I have a device ID of 123, I think they're more complicated than that, but if there's a device ID number of 123, and device ID No. 123 is swept up in geofence warrant one, if I see device ID No. 123 in geofence warrant No. 2, does that mean that that is the same device?

A Based on reading her declaration, I believe so.

Q Is there any obligation that the law enforcement officers who obtain the returns from Google have to return the data after they have used it in any way?

A I'm not aware of any.

Q Okay. Let's talk now about some of the questions that Mr. Duffey was asking you about your follow-up investigation. As a former law enforcement officer, were you a detective?

A I was.

Q And as a detective, is it your job to do police work and follow-up work?

A That's what I did.
Q Such as get search warrants?
A Yes.
Q And do surveillance?
A Yes.
Q And try to track people down from various location data points?
A Yes.
Q Were you successful in doing that?
A I believe so.
Q Is that the nature of detective work is you have to actually do the work?
A It is. I mean, connecting the dots is what you do.
Q Obviously, law enforcement officers would like their jobs to be easier; right?
A Sure.
Q But there are sometimes stumbling blocks?
A There's work to be done.
Q But you still have to work around that?
A Yes.
Q When we were talking in advance of today, do you have an example of two data points that would apply to you today but nobody else probably?
A Yeah. I recall you asking me this before, and I

kind of used the example of me coming here today.
Q How would that work?
A I think I'm the only person. I haven't seen any of my neighbors, but I think I'm the only person from my cul-de-sac who traveled from Holly Springs, North Carolina, to the federal courthouse today. I don't think there's anybody else. So those two points would be --
Q Sufficient to identify you?
A Yes.
Q Okay. And, obviously, the more points of data you have, is it more likely that you're going to get a precise narrowing down of who the identity is of that person that's carrying that device?
A Can be. With what I do, more data is -- we always want more data. It helps everything when you can -- the more you know.
Q I want to turn now to the screens that we were talking about. So if we go to Mr. McGriff's affidavit. And so this is Defense Exhibit 23 at page 3. If you can turn to that exhibit, please.
A Say that again.
Q Defense Exhibit 23 at page 3.
I'm sorry. So on Footnote 2 of page 3, Mr. McGriff refers to, like, a second screen; right?

A Yes.
Q And have you been able to determine that -- and if we look up, we see on that above, that page flips into paragraph 8 of Defense Exhibit 23. And that portion has the Location History in bold, and then under that it says "Saves where you go with your devices"?
A Yes.
Q And then under that it has "Location History. Saves where you go with your devices"?
A Yes.
Q And so when Mr. McGriff seems to be talking about the second screen, we've been able to determine, is that really just the language that's under the drop down arrow?
A That's what it looks like. This language that you see in this under No. 8 is the same that we saw in most of the other screenshots that actually show the expansion arrow selected.
Q Because when Mr. McGriff is writing this, he's indicating I don't have the screenshots -- right? -- of activating this? And so I'm describing what language would have been presented?
A I don't believe so. I don't think he turned over -- I think that's correct.
Q And so when we see the "Saves where you go with

your devices" language in the examples that you have put forth in Defendant's Exhibit 7, all the user has to see under Location History is "Saves where you go with your devices," in the Norwegian example, specifically, and then they can click yes, and that will turn on?

A Yes, you can.

Q And that's it? You don't have to look at any of that other expansion arrow?

A You don't have to, no.

Q And going back to -- I just want to make sure I'm, again, clear about turning on Google Assistant. So if I have my phone. I just push that little circle button at the bottom; right? That's the home button?

A Yeah, I believe that's the icon that's used.

Q And you just hold it and press it for a couple of seconds?

A It's not even really a couple of seconds. It's more of just, you know, if you were clicking on something on a website, how you normally just tap the screen. This is more of just a press, a longer version of that touch.

Q And so if you're doing that for the first time, and you haven't already activated Google Assistant, it's going to take you to the setup process; right?

A From what I've seen, yes.
Q And then when you're doing that, you either have to choose yes, I'm going to do it or no, I'm not going to do it to turn on Google Assistant?
A Right. You either "Skip" the setup of Google Assistant or you go "Next," and have to choose permissions.
Q So you just have to do two clicks; right? The long press of the home button and then the "Yes, I'm in"; right? You just have to do two clicks; right? Or two presses or two movements of your hand?
A I guess it would actually be three.
Q What would the movements be?
A You're long pressing to launch the app. When that comes up, then you see the "Meet your Google Assistant" screen. You can select "Skip" or "Next." If you select "Next," it takes you to the permission screen where you have to make the selection of "Turn on" or "No, thanks."
Q So, thank you for correcting me. So it's three presses, and that could happen within probably less than a second; right?
A I guess, yeah, you could.
Q Okay. Is it pretty easy to turn on Google Assistant, then?

A Yeah, it can be.
Q And anywhere in the screens that have you found in the research of what the screens themselves would have looked like to a user setting up Google Assistant on July 9th of 2018, does it indicate that deleting information, that if you accept Location History, does it ever indicate that deleting your information doesn't stop you from tracking information in the future?
A I'm not sure. Ask that again.
Q So if we go down to the drop down menu, your location history. And the bottom says -- I'm sorry. Not that. Not that portion. The -- so the paragraph that's right above the boxes that say either "No, thanks" or "Turn on." So this is on page 4 of Exhibit 7, which is the second set of the July 2, 2018 screenshots from the Norwegian Consumer Council.
A Yes.
Q That paragraph that begins "This data may be saved and used in any Google service." And the second sentence says that you can delete the Location History data; right?
A Yes.
Q Does that in any way indicate that if you delete the Location History data, that it will still keep

tracking Location History data in the future?
A No, I don't think it indicates that it won't. If just by simply deleting your old location history, no, I don't think that indicates that it will stop collecting more information.
Q But if I were -- like, if I had Location History enabled, and I deleted at this time my location history, would it still keep tracking my location history even if I deleted the old information?
A If you allow it to continue to be enabled, then, yes, it would.
Q But there's no -- when you delete it, is there a portion of the deletion information that tells you that you are not going -- that location history information will still continue to be gathered from you?
A I'm not aware that that's the way that it's displayed, but deleting it is not going to stop it from -- deleting your old history is not going to stop it from collecting.
MS. KOENIG: If I can have just a moment, Your Honor.
No further questions, Your Honor. Thank you.
THE COURT: All right. Can this witness be excused?

MS. KOENIG: He may, Your Honor.

THE COURT: All right. Excused excused or subject to recall?

MS. KOENIG: Subject to recall, Your Honor, by the defense.

THE COURT: All right, sir. You may stand down. Thank you for your testimony.

Because you might be subject to recall, it's still as if you're testifying. You can't talk to anybody about what you've testified to or what anybody else has testified to. Thank you.

(The witness was excused from the witness stand.)

MS. KOENIG: Your Honor, if we could take a brief break before we begin the next witness.

THE COURT: Yes, I think it's a good time to do that. So we could go -- we'll go until just five minutes of three. That's a little more than 15 minutes.

MS. KOENIG: Thank you, Your Honor.

THE COURT: So we'll take a recess. Again, nobody violate our sequester order that continues to be in place. All right? Thank you.

(Recess at 2:35 p.m. to 2:55 p.m.)

THE COURT: All right. So we're returning

from our break. I need to, if we have folks online to remind them that our Local Rule Criminal Rule 53 prohibits, and our standing order, prohibits anybody from recording or broadcasting or telecasting these proceedings. It is as if you are in court with us. And we have one court reporter making our official record.

So I understand we have a new witness, who is actually in the witness box, but who needs to be called and sworn. Right?

MR. PRICE: Thank you, Your Honor. The defense calls Marlo McGriff to the stand.

MARLO MCGRIFF, called by the Defendant, first being duly sworn, testified as follows:

THE COURT: All right. Mr. McGriff, we are adhering to COVID protocol here. Obviously, you can see we have plastic barriers. We're not within 6 feet of each other unless folks have taken necessary precautions. You have sanitizer there and hand sanitizer.

When you're testifying, the only way that my court reporter can hear you is through the microphone. So you can either testify with or without a mask. I

just want to be sure that it is going through the microphone so we can hear you clearly. All right, sir?

THE WITNESS: Okay.

THE COURT: All right. Thank you.

MR. PRICE: And, Your Honor, I just wanted to remind the Court that we have agreed to treat Google's witnesses, including Mr. McGriff, as adverse in this case.

THE COURT: All right. I do need to remind you all of one thing. On the break, I was notified that I have to attend an important conference call at 5 o'clock. And so we're going to have to break before 5 o'clock. Otherwise, I wouldn't do it, but it is apparently enough that we have to take a break. So we will be doing that, just to give you the advance notice.

MR. PRICE: Understood. Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. PRICE:

Q Mr. McGriff, hi. Good afternoon. I'm Michael Price. I'm an attorney with Mr. Chatrie. Thank you for being here today.

You are a Location History Product Manager for Google?
A That's correct.
Q And that means you're responsible for the Location History product?
A That's correct.
Q And you've had that position since 2016?
A That's correct.
Q And you joined Google in 2011?
A Yes.
Q So you're very familiar with Google?
A That's correct.
Q And you're very, very familiar with Location History in particular?
A Yes.
Q So you've helped develop it for the last five years?
A That's right.
Q And now you lead the cross functional location history team?
A That's correct.
Q So that means you're not just familiar with how Location History works, but how it works with Google's other services?
A That's correct.

Q And does that include Google Assistant?
A Some aspects of Assistant, yes.
Q And you filed three declarations in this case; correct?
A That's correct.
Q Your first on March 11th, 2020?
A I believe so, yes.
MR. PRICE: Can we bring up Defense Exhibit 1.
Q This is the first declaration that you filed in this case?
A Yes. You said this is Exhibit 1?
Q Yes. It has previously been admitted, and it's Defense Exhibit 1.
MS. KOENIG: 21.
THE COURT: 21.
MR. PRICE: 21, I'm sorry.
Q Okay.
A Yes.
Q Great. So Location History was not initially designed to assist law enforcement investigations, was it?
A That's correct.
Q It was designed to support Google's Timeline feature as you explain on page 9?

THE COURT: Are we entering this into evidence?

MR. PRICE: It is already in evidence, Your Honor.

THE COURT: No, it's not. No. 3 is in evidence.

MS. KOENIG: I have Exhibit 21 is admitted into evidence with Mr. McInvaille, Your Honor.

THE COURT: Oh, it sure is. My apologies. It's 22 that isn't. My apologies.

A That's correct. It mentions, if I'm looking at page 9, it mentions Timeline as a feature, yes.

THE COURT: So, sir, I didn't hear a word of that. So I think the microphone needs to be a little closer to you. And it's natural when you're sort of looking away from the document at the document that you also turn away from the microphone. It's an unnatural way to speak, but we want to be sure that we get it accurately. All right?

THE WITNESS: Okay. Sorry about that.

BY MR. PRICE:

Q So could you repeat that answer? Location History was designed to support Google's Timeline feature; correct?

A That's correct.

Q And as you wrote in your first declaration, also on page 9, "The purposes for which Google designed Location History do not depend on any individual stored Location History data points"?

A That's correct.

Q In other words, Google can infer where a person is heading with their device even with a few points registering along their path?

A I'm not sure that I follow that question.

Q Google uses Location History to infer a user's location; correct?

A I wouldn't use it -- I wouldn't frame it in that way, but various signals are used to infer where a user is. That's how we infer a user's location. And then those inferences are stored, which create the history.

Q Sure. And if somebody is traveling along a path, and one dot is kind of off out of the way, Location History will snap that point right back onto the path; correct?

A Only if it makes sense. We do filter out like an outlier because that sort of teleportation can happen.

THE COURT: That sort of what?

THE WITNESS: Sorry. There can be an outlier point. But, logically, if I was here, and then

there's one point I'm sitting in -- let's say I was sitting here for an hour. And there's one point that's not where I've been sitting for the hour. That's an outlier point, but yes.

Q My point is, it's precise enough for what it was designed to do for Timeline?

A That's correct.

Q And that's why you wrote, "Location History" -- this is also on page 9, Slide 2, this is why you wrote, "Location History is sufficiently precise and reliable for these purposes for which Google designed Location History"; correct?

A That's correct.

Q That indicates, though, that there's maybe more than one purpose for Location History; correct?

A Yes.

Q Another purpose of Location History, as you wrote in the same paragraph, is to serve ads based on user location?

A Yes.

Q And for some advertisers you also provide information about store visit conversions; is that true?

A That's correct.

Q Could you explain what store conversions are?

A So, for Location History, we never share anyone's location history with a third party. So there's no instance where you would share with a third party that I went into a particular store. What Location History is used for in terms of advertising is very specifically ads measurement. And so that is for a particular campaign, how many users who saw a particular ad actually went to one of those stores. And that's the store visit conversion or ads measurement you're referring to.

THE COURT: Okay. You're just talking too quickly. I'm so sorry.

THE WITNESS: I'm sorry.

THE COURT: It sounds as if that's the way you normally talk, but pretend like I'm three, and slow down a little, if you don't mind.

THE WITNESS: Yes, absolutely.

BY MR. PRICE:

Q So Google is doing this in a privacy protective way; correct?

A That's correct.

Q It's not giving user location data over to stores about who was around?

A No.

Q And businesses can also use Google to target ads

based on a device's location?
A Not using Location History, though.
Q Right. They're not using the user's thing. They're going to Google, and they're attempting to target ads based on geography?
A Yes.
Q Okay. In fact, it's possible to do something called radius targeting; is that true?
A Yes, but I'm not totally familiar on the full ad suite of products.
Q My understanding is that it allows a business to target ads to users that are within a certain distance of that business.
A That sounds correct, yes.
Q And there's a minimum radius that advertisers can select when doing that; right? You can't make your radius 4 meters or something like that?
THE COURT: Okay. Now you're also fading out.
There you go.
MR. PRICE: Sorry.
BY MR. PRICE:
Q There's a minimum radius that advertisers must adhere to. They can't select I believe it's less than a kilometer or less than a mile radius?

A That sounds correct.
Q And those businesses don't actually get to see which devices are in the area; correct?
A Not that I'm aware of, no.
Q And the businesses can't go back to Google and ask for more information about where a particular user was half an hour before or half an hour later?
A No.
Q They can't get any information at all about individual users; correct?
A Not that I'm aware of, no.
Q And that's true even when you're tracking store visit conversions, no exceptions?
A That's correct.
Q So Google filed an amicus brief in this case. Are you aware of that?
A Yes.
Q You're probably familiar with it. You probably helped put it together?
A Yes.
MR. PRICE: I'd like to bring up Defense Exhibit 2.
Q Is this the amicus brief?
A Which --
Q It's also on your screen as Defense Exhibit 2.

A I don't think my screen is actually updating. It's been static on the same --

MS. KOENIG: It is different, but they are white papers with letters on them.

THE WITNESS: Maybe it just looks the same.

BY MR. PRICE:

Q It should say "Brief of Amicus Curiae Google LLC."

A I see it. Thank you.

Q So that's the amicus brief that Google filed that you helped prepare?

A Yes.

MR. PRICE: I'd like to admit that into evidence, Your Honor.

THE COURT: No objection, right?

MR. SIMON: No objection, Judge.

THE COURT: It will be admitted for purposes of the hearing, too.

MR. PRICE: Thank you.

(Defense Exhibit No 2 is admitted into evidence.)

BY MR. PRICE:

Q So on pages 5 to 6, Slide 4, the brief goes out of its way to correct a misconception in this case; correct?

A That's correct.

Q Google says that a geofence warrant is not really analogous to a so-called tower dump?

A Yes.

Q And the brief states, "In fact, while Google Location History information bears some similarities to those types of data in some respects, it is different in important ways that are highly relevant"; right?

A Yes.

Q And it goes on to explain, with respect to cell site location information, which is how tower dumps work, "When law enforcement seeks access to CSLI," cell site location information, "it is thus asking the wireless carriers to produce its own business records showing when a particular device connected to a cell site within a particular period of time. A request for a tower dump likewise seeks the wireless carrier's own business records. In that case, identifying every phone that connected to a particular cell site or tower in a particular period"; correct?

A Yes.

THE COURT: What page are you on?

MR. PRICE: That is page 9, Your Honor.

THE COURT: Thank you.

BY MR. PRICE:

Q And there are only so many people that can connect to one cell tower at a time; right?
A That's correct.
Q And so there's sort of an upper limit on the number of users that can be searched as a result of a tower dump?
A That I don't know.
Q Well, if you're choosing, say, three towers to search, and there's a maximum number of people that can be on one tower at a time, would you agree there's a maximum, there's a cap?
A That has to be some cap, yes.
Q There's a natural limit?
A Yeah.
Q And that would be true even if the tower dump involved more than one tower. There would still be that sort of upper limit. And that differs from how geofence searches work; right?
A That's correct.
Q That's because -- and this is on page 8 of your first declaration, which is Exhibit 21, Defense Exhibit 21. You explain that's because, unlike tower dumps, Google does not know which users may have saved Location History data before conducting the search and running computations; correct?

A That's correct.
Q And going back to the amicus, and I apologize for the -- this is Slide 7 at page 12. Google says it "has no way to know ex ante which users may have Location History data indicating their potential presence in particular areas at particular times"; is that correct?
A That's correct.
Q So, unlike a tower dump, there is no way of just searching Location History records for people in one area in the way that you do with a tower dump by looking at a tower?
A That's correct.
Q You have to search all of the records for every user with Location History enabled; right?
A Yes.
Q And this is at your first declaration, page 8, Slide 8. You say in your first declaration, To conduct a geofence search, Google must search across all Location History data to identify users with Location History data during the relevant time frame; correct?
A Yes.
Q And you then have to run a computation against every set of stored Location History coordinates to

determine which records match the geographic parameters in the warrant?

A Yes.

Q And then, as Google explains in its amicus, similarly, page 12, "In order to comply with the first step of the geofence protocol, therefore, Google must search across all Location History journal entries to identify users with potentially responsive Location History data, and then run a computation against every set of coordinates to determine which Location History records match the time and space parameters in the warrant"?

A Yes.

Q So for every geofence warrant, Google has to search across all Location History journal entries, and then it has to run a computation against every set of coordinates; correct?

A Yes.

Q In other words, you had to search everybody with Location History enabled?

A Yes.

Q That's what happened in this case?

A Yes.

Q To look for users in the geofence provided by the warrant, Google had to search literally everybody with

Location History enabled?
A Yes.
Q I want to try and figure out just how many people had their data searched in this case. So Google searched all accounts with Location History enabled, and in your first declaration -- this would be the fourth page, paragraph 13 -- you say, In 2019, roughly one-third of active Google users, i.e., numerous tens of millions of Google users, had their Location History enabled on their accounts?
A Yes.
Q Numerous tens of millions. That's a lot.
A Yes.
Q Can you tell us precisely how many?
A At that point in time, I cannot.
Q Let's try it a different way. Google owns Android; right?
A That's correct.
Q And you know that Android has a Twitter account?
A I'm certain they do, yes.
Q And occasionally it tweets updates about Android. Yes?
A Yes.
Q And in May 2019, Android said they had 2.5 billion active users; is that accurate?

A I have not seen that tweet.
Q Well, I believe we can show it to you. It's Defense Exhibit 55.
A The tweet says 2.5 billion active devices. It doesn't speak to accounts.
Q As a rough estimate, would that differ significantly from the number of users?
MR. SIMON: Judge, I'm going to object. He's answered the question. He said he doesn't know. The pressing on, I think particularly given the time constraints, the witness had answered the question to the extent he has personal knowledge.
THE COURT: Just finish answering that question and we will move on.
A I wouldn't be able to say.
Q Okay.
THE COURT: Are you moving that into evidence or not? Is it just demonstrative?
MR. PRICE: It was just demonstrative, Your Honor.
BY MR. PRICE:
Q If you had to take a rough estimate at the number of active users in 2019, do you think it would be much different than 2.5 billion?
A I would not even know where to begin to make that

assessment.
Q So you don't know how many people have Location History enabled? I mean, presumably, you said you're in charge of the Location History product.
A Yes. If the question is how many users were opted in to Location History in 2019, I do not know that number off the top of my head. My clarifying questions would be at a particular point in 2019, because it's not a static number? Or were you just looking for a rough range or average? But, again, I wouldn't know that off the top of my head.
I remember at the time of preparing this that it was roughly a third, the Android number, but I do not know the Android number again off the top of my head.
Q And if we take, for example, if we say 2.5 billion as the Android number, a third of that would translate into about 800 million, just generally.
A The Android number here was referencing devices, though. I, for example, have multiple devices, but only one account that I'm using across all those devices.
Q In your estimation as the Location History Product Manager, would you estimate that there were more or less than 800 million users with Location History enabled at some point in 2019?

A Users as in they have the account on, Location History on, or Location History on and actively reporting?

Q Enabled on their accounts.

A That I couldn't say. That I couldn't say.

Q Okay. In any case -- all right. We'll move on.

I want to talk about how Google processes Location History geofence warrants. When Google receives a geofence warrant, what happens? What is the process?

A I'm not involved in the processing of the warrants in any way.

Q Do you know if there are any rules that Google has about the size of a geofence warrant?

A I know at a high level the team works to be sure -- at a high level I know that there's some back and forth in terms of the refinement of the request, but I'm not involved in the details of that refinement.

Q What do you mean, back and forth about the refinement of a request?

A Just clarification. Do we have the right details? There's some process. I believe there's someone else who's a witness who can speak to it in detail, but I'm not involved in that process at all.

Q So you don't know if there's an upper limit on the

size of a geofence that Google would respond for?
A I am not involved in that at all day-to-day.
Q If we asked for all the data in a city over a two-week period, would Google comply with that?
A I can say with certainty they likely wouldn't, but I have no idea what their parameters are for that.
Q Do you know what the rules are for narrowing things down at each stage of the process?
A I do not.
Q So when the government comes back in Stage 2 and says, Well, you know, we want all of them, do you know if that's okay or not?
A Again, my knowledge and involvement with that process is limited to something is wrong in their processing, and there's an ask to understand why some particular aspect of retrieving whatever they've decided fits within scope is not retrieving in the way that it should.
Q What do you mean "not retrieving in the way that it should"?
A That there's some delay or some sort of just general process breakdown. I'm often engaged to -- not often, but when it happens, I'm engaged to assist with looking into the issue, but, again, I'm not involved in either the receipt of or the processing of

or the response to.
Q Okay. You're aware that Google has notified some users when they've been the subject of a geofence warrant; right?
A That's correct, yes.
Q You're aware that just recently Google notified a Minneapolis user who is the subject of a geofence warrant targeting protesters following the death of George Floyd?
A I was not aware of that, no.
Q Were you aware that Google notified a user in Florida who is the subject of a geofence warrant from the Gainesville Police Department?
A I was not aware of that, no.
Q In which cases are you aware of Google notifying users of a geofence warrant?
A I am not involved in any way in the day-to-day processing of geofence warrants, their receipt, any responses. That is not involved in my day-to-day whatsoever.
Q Are you aware that Google never notified Mr. Chatrie that he was the subject of a geofence warrant in this case?
A I would not be able to comment on that.
Q I assume you don't know, then, the rules for when

Google will notify users that they are the subject of a geofence warrant?

A I do not know that, I'm sorry.

Q Okay. I want to go back to your first declaration, page 7. It says, "Location History is the only form of location data that Google maintains that Google believes to be responsive to a geofence request"?

A That is correct, yes.

Q And Location History is the only form of location data that was produced to the government in this case?

A To my knowledge, yes.

Q So no Google Location Accuracy data, no Web & App Activity data?

A No.

Q And the reason for that is because only Location History -- well, let me take a step back. When the government makes a geofence request, does it specify that it wants to search only Location History?

A I don't believe so.

Q And Google does actually maintain location data apart from Location History in Web & App Activity, for example?

A Some location information can be captured in Web & App Activity, yes.

Q But Location History was the only repository of location data that Google searched in this case?
A Yes.
Q That's because only Location History is sufficiently granular to be responsive and searchable?
A That is my understanding, yes.
Q And only Location History is able to pinpoint a user's estimated location with enough precision?
A That is correct.
Q So Google decided that only Location History was precise enough to be searched in response to a geofence warrant?
A That is my understanding, yes.
Q Okay. Now, even though you said pinpoint, and this is page 8 of your declaration, the location data points reflected in Location History are really estimates; is that right?
A That's correct.
Q A user's actual location doesn't necessarily align perfectly with any one isolated data point?
A Yes.
Q There's a confidence interval, a number associated with each set of Location History coordinates that reflects Google's confidence in those coordinates?
A Yes.

Q And this number is expressed in meters as a radius?
A Yes.
Q And it's called the display radius; is that correct?
A Yes.
Q So it can be visualized as a shaded circle around the coordinates?
A Yes.
Q The magic blue circle around the blue dot?
A Yes.
Q And on pages 8 to 9, you say Google aims to accurately capture roughly 68 percent of users with this method?
A Yes.
Q Or, in other words, there's a 68 percent likelihood that a user is somewhere inside of that shaded circle, or at least that's Google's goal?
A Yes.
Q That means there's a 32 percent chance that they're outside of that circle altogether?
A Yes.
Q Not necessarily at the blue dot?
A Yes.
Q Is it just as likely that the user's actual

location would be near the edge of that circle as opposed to smack dab in the middle?

A Yes.

Q So you're equally confident -- you're confident that the user is in that circle, 68 percent, but where you put those coordinates doesn't necessarily translate into that same amount of confidence. You're still only 68 percent confident?

A That the device is within those coordinates, yes.

Q Okay. So, moving on to page 9, you stated that if the estimated location, the stored coordinates in Location History, falls within the radius of the geofence request, then Google treats that user as falling within the scope of the request; correct?

A Yes.

Q So, in other words, if the blue dot is inside of that geofence, inside of that radius, then Google will consider it responsive to the warrant?

A Yes.

Q You consider it responsive even if that shaded circle, the confidence interval display radius, falls partly outside the radius of the geofence request?

A That is my understanding, yes.

Q So you can have a little blue dot right close to the edge of that geofence with a big display radius

that goes way beyond it, and that user is still going to be recorded in the geofence return?

A Yes.

Q So you consider it responsive even if the shaded circle falls partly outside? And even then, you can't say where inside that circle the user was?

A No.

THE COURT: What question did you answer? He asked two questions. Do you think if it's outside the circle, it's responsive?

Why don't you rephrase the question.

BY MR. PRICE:

Q So even if part of that display radius falls outside of the geofence, it's still considered responsive?

A Yes.

Q Even though there's a 68 percent chance that that person is somewhere outside the actual geofence within that display radius?

A Yes, that would still be considered responsive.

Q Even though there's a 32 percent chance that they're not even there and somewhere else?

A Yes.

Q Okay. So there's a significant likelihood that at least some of the users identified as being inside the

geofence might have been outside of that geofence?
A There is a possibility, yes.
Q Google has to draw the line somewhere; right? And this practice makes sense from Google's perspective?
A This is the process, yes.
Q The warrant didn't tell you to do it this way; right?
A This is the process by which we respond to these, yes.
Q It's Google's process. It didn't tell you to do this in the warrant?
A (Nodded head affirmatively.)
Q And no court told you to do that; right?
A This particular process of identification?
Q Yeah, to draw the line and say, well, we're going to report people whose blue dots are inside, and that's the way it's going to work.
A This is the process that we use to respond to these, yes.
Q Okay. So false positives are possible here?
A Yes.
Q And you say this, page 9 of your first declaration, 17. You said, "As a result, it is possible that when Google is compelled to return data in response to a geofence warrant, some of the users

whose locations are estimated to be within the radius described in the warrant, and whose data is therefore included in data production, were in fact located outside the radius"?

A Yes.

Q False negatives are possible, too; right?

A Yes.

Q So if somebody was standing -- if somebody was actually right outside that geofence radius, but Google estimated their location as being inside of it or, I'm sorry, other way around. If the blue dot falls outside the geofence, you don't include it even though the person could have been inside of that geofence?

A That's correct.

Q Okay. Even if part of the shaded circle falls within the geofence, if that blue dot is outside, nothing?

A Yes.

Q The warrant, once again, didn't tell you to do it that way?

A This is our process, yes.

Q The Court didn't tell you to do it that way?

A This is our process, yes.

Q It's just your process. Great.

All right. I want to switch gears a little bit here and talk about some of the feedback that Google has received about Location History. You published a blog for Google on December 9, 2019; correct?

A Yes.

Q It was titled "Updates to Incognito Mode and Your Timeline in Maps"?

A Yes.

Q Let me show you Exhibit 47. Is this the blog post?

A Yes.

MR. PRICE: Your Honor, I'd like to introduce this into evidence, please?

THE COURT: Any objection?

MR. SIMON: No objection, Judge.

THE COURT: It will be entered.

MR. PRICE: Thank you.

(Defense Exhibit No. 47 is admitted into evidence.)

BY MR. PRICE:

Q So you wrote --

MR. PRICE: This is on 19, Laura.

Q You wrote that throughout this year, we've focused on making it easier to control, manage, and delete your Location History information; correct?

A Yes.
Q And earlier that year, same year, you published another blog post for Google. This one on May 1, 2019.
A Yes.
Q It was titled "Introducing Auto Delete Controls for Your Location History and Activity Data"?
A Yes.
Q Is this the blog post?
A Yes.

MR. PRICE: Your Honor, this is Defense Exhibit 46. We'd like to move it into evidence, as well.

THE COURT: Any objection?

MR. SIMON: No objection.

THE COURT: It will be entered.

(Defense Exhibit No. 46 is admitted into evidence.)

Q So you wrote, "We work to keep your data private and secure, and we've heard your feedback that we need to provide simpler ways for you to manage or delete it"; correct?
A Yes.
Q I would like to talk about some of that feedback for a second that you received. In fact, Location

History has received some significant media attention and received significant media attention in 2018; is that correct?

A Yes.

Q And that attention was pretty negative?

A It was mixed, yes.

Q In January 2018, there's an online type magazine called "Quartz," and they published an article discussing Location History. Do you mean that?

A Yes.

Q It was titled, "If You're Using An Android Phone, Google May Be Tracking Every Move You Make." This is the article?

A Yes.

MR. PRICE: This is Defense Exhibit 48, Your Honor. And I would like to move it into evidence.

MS. KOENIG: It already is in evidence.

MR. PRICE: It already is in evidence. Thank you.

Q So speaking of Location History, it says, "Although the product behind those transmissions is opt-in, for Android users it can be hard to avoid and even harder to understand"; correct?

A Yes.

Q And it goes on to say, "While it is not enabled on

an Android phone by default, or even suggested to be turned on when setting up a new phone, activating Location History is subtly baked into setup for apps like Google Maps, Photos, the Google Assistant, and the primary Google app"; correct?

A Yes, that's what the article says.

Q And then it adds --

THE COURT: There's an objection.

MR. SIMON: Judge, I just object to the way in which this is being entered into evidence, particularly that first sentence. I didn't object at the time, but the way the record is going to read is that Mr. McGriff is saying that he agrees with this. I would prefer, Judge, and I think the record would be clearer, if he's going to put these assertions in front of the witness, ask him to assess them.

THE COURT: At the very least --

MR. PRICE: Your Honor, I am not -- sorry.

THE COURT: Okay. You can respond.

MR. PRICE: We are not introducing these articles for the truth of the matter. We are introducing them because they constitute feedback which Google received.

THE COURT: I know, but what you're doing is saying that the declarative statements, and you're

starting it by saying "It says this. Is that right?" He says yes. It's going to create a record where you can cut off the front where you say it says this, quote it, and then say yes.

So what we're trying to do is create a fair record here. You are getting him to indicate that there are statements in this article and whether or not he knew them. And so that is really the point.

I would agree that this way it's being asked, it sounds as if you're trying to get him to, although you're not doing it that way, but it does sound as if you're trying to get him to sound as if he's agreeing with a declaration.

So it's sustained to that degree. And I'll just ask you to use the nuances. You're still making your point. But do it in a different way.

MR. PRICE: Okay.

BY MR. PRICE:

Q The article here criticized Location History; correct?

A Yes.

Q And the article looked at testing multiple phones to see what this process was like; correct?

A Yes, it did.

Q And it faulted Google, didn't it?

A The article did, yes.
Q And it faulted it because it said that none of the apps used the same language to describe what happens when Location History is enabled; correct?
A That is one of the things they cited, yes.
Q And it also criticized Google for not explicitly indicating that activation will allow every Google app, not just one seeking permission, to access Location History data. So they're complaining about account level nature of the setting.
THE COURT: The what?
MR. PRICE: Account level nature of the setting.
THE COURT: You need to look at the microphone.
A Yes, they are in the article.
Q Okay. And that account level setting, that means that when you turn on Location History through one app, it's on for the entire account; right?
A When you opt in to Location History, you are opting in for your account, yes.
Q Thank you.
So the press didn't stop with the Quartz article. I imagine you're aware that the Associated Press also published an article about Location History in 2018?

A Yes, I am aware of that article.
Q Is this the article?
A That is the article, yes.
Q It's titled "Google Tracks Your Movements, Like It or Not"?
A Yes, that's the title of the article.
Q Thank you.

MR. PRICE: And this is Defense Exhibit 49, Your Honor. And we would ask to move this into evidence, as well.

THE COURT: Any objection?

MR. SIMON: Judge, we just reiterate our earlier objections. We think it lacks relevance, particularly when you have a Google witness here to address the issue. It's obviously hearsay. Understanding that the rules of evidence wouldn't strictly apply here, but I think the best route here is to question the witness about, like, the Quartz article assertions. But I know the Court has previously ruled, but we'd object to it being entered into evidence.

THE COURT: Right. He's allowed to make his case. I will allow it for the limited purpose, not for the truth of the matter, but to the extent it has -- the witness has already testified that he was

aware of the article. And so I think it is relevant for background information. And you all can cross-examine with respect to weight. All right?

MR. SIMON: Understood.

MR. PRICE: Thank you, Your Honor.

Sorry. I did move to have the article introduced. I'm not sure if there was a ruling on that, Your Honor.

THE COURT: Right. I overruled the objection, and so it will go in.

MR. PRICE: Thank you.

(Defense Exhibit No. 49 is admitted into evidence.)

BY MR. PRICE:

Q So the article's main complaint here is that it says, "Even with Location History paused, some Google apps automatically store time-stamped location data without asking." That's just the complaint in the article; correct?

A That's the complaint in the article, yes.

Q But it was a complaint that Google ended up taking pretty seriously, especially given the interest from members of the Senate, for example?

A We take all complaints seriously, yes.

Q Here the article actually quoted United States

Senator Mark Warner; correct?
A Yes, the article does quote the Senator.
Q And he complained that it's frustratingly common for technology companies to have corporate practices that diverge wildly from the reasonable expectations of their users. Was that his statement?
A That was his statement, yes.
Q You were aware that he made that statement; correct?
A I was aware that he made that statement, yes.
Q And at the end, it quotes a Yale researcher, Sean O'Brien, and he called this practice disingenuous; right?
A That is what he said, yes.
Q So this was a pretty negative report about Location History from Google's perspective; correct?
A It was not a flattering report, that's correct.
Q Google actually tracked the media coverage of this report; correct?
A As we do often for all media reports, yes.
Q And Google prepared what's called an issue coverage report for this article for four days?
A That's correct, yes.
Q I'd like to show you Defense Exhibit 38, please. Are these the issue coverage reports that you were

referring to?
A That's correct, yes.
Q And it makes it clear that this story was pretty widely covered; correct?
A That's correct, yes.
Q If we check out one of those reports --
THE COURT: What exhibit are you on?
MR. PRICE: Sorry. Excuse me?
THE COURT: Which exhibit?
MR. PRICE: Sorry. This is Defense Exhibit 38, Your Honor.
THE COURT: 38?
MR. PRICE: Yes. And I forgot to move it into evidence. I would move for this to be admitted into evidence, as well.
THE COURT: Is there any objection to Defense 38?
MR. SIMON: No objection, Judge.
THE COURT: All right. It will enter.
(Defense Exhibit No. 38 is admitted into evidence.)
BY MR. PRICE:
Q So if we look at the issue coverage reports, we see that Google wrote, the AP tweeted the story out, which created a surge of social chatter, approximately

8,000 re-tweets. And the story was picked up by 60 plus outlets, including the *New York Times*, *U.S. News and World Report*, and the *Washington Post*; is that accurate?

A That's accurate.

THE COURT: It's accurate that it's in there. You're continuing to ask the questions in the same way. And so, you know, you're making points, but you are making the points. It's the witness who needs to be able to talk about what it is that is or is not in an exhibit.

That is what is in the exhibit.

MR. PRICE: Thank you, Your Honor.

BY MR. PRICE:

Q Google's report explained the coverage themes for these stories; is that correct?

A That's what's in the report, yes.

Q And the report noted the top two themes for this article? It said, the report said, that 69 percent of the coverage mentioned the lack of user consent/creepy factor?

A That's what is in the report, yes.

Q And the report also noted that a third of the coverage was about misleading controls?

A That's in the report, yes.

Q Just a few days later, Google changed the language on its help page. On its Location History help page. You're aware of that, I assume?

A Yes.

Q It was in response to this article; is that correct?

A Which update are you referring to specifically? Is it an exhibit here?

Q It was three days later. And that would have been on August 17, 2018.

A Is there an exhibit here I can look at?

Q Yes. We'll get there.

So three days later -- sorry -- three days later it was reported that Google changed its Location History help page, as well; is that correct?

A I can't say that we made an update three days later.

Q The Associated Press published an article just a few days later about that change. Are you aware of that?

A Is that in this book?

Q We can show you the article if you'd like. Would that help?

A Well, I guess, the Associate Press reported that we made -- that Google made a change three days later.

Q Yes.
A So if that's in there, yes, then that is what they reported.
Q And you do recall Google making a change to its Location History help page shortly after this article?
A I recall in some period of time, yes, we made updates to our pages.
Q Okay. That's fine. The bad press, so to speak, here had some ramifications for Google in terms of oversight from the federal government; is that correct?
A It did.
Q In May 2018, are you aware that two United States Senators wrote a letter to the Federal Trade Commission about Location History?
A Yes.
MR. PRICE: And this is 36, Laura.
Q Is this the letter?
THE COURT: Okay. Is this Defense Exhibit 36?
MR. PRICE: This is Defense Exhibit 53, Your Honor.
THE COURT: Okay.
Q I'd like to show you what's marked as Defense Exhibit 53. It's a letter from two United States

Senators; correct?

A Yes.

MR. PRICE: Your Honor, I would like to move this letter into evidence.

THE COURT: Any objection?

MR. SIMON: Judge, I think there are multiple letters in Exhibit 3 (sic), including Google's response on January 12, 2018. We'd obviously object generally based on what we've talked about before, but I understand the Court will admit it not for the truth of the matter asserted, but for -- just to allow the question.

THE COURT: All right. I'm going to allow this for the limited purpose that we have been looking at these documents.

So, to make a record, this is Defense Exhibit 53, which is a letter dated May 11, 2018, that has a signature of Richard Blumenthal from the United States Senate.

It then has something marked an attachment. And the attachment says "Letter from Susan Molinari. Received by Senators Blumenthal and Markey." And that is then followed by a January 12, 2018 document on Google letterhead. So it predates this May 18th letter.

And then there is something that has an Attachment 4. So you have to be clear about what you're admitting and under what circumstances.

The United States is correct that it's confusing to say we're admitting just one letter. There's actually a series of documents here.

So you can ask questions to establish why they're there, but the whole -- what so far we have admitted is part of 53, the May 11, 2018 letter.

MR. PRICE: Yes, Your Honor. Thank you. And the exhibits that go along with it include previous correspondence. There's one in particular that we have an interest in. It's Attachment 4, which includes a screenshot of the Google Assistant setup.

THE COURT: There is no Attachment 2, letter from Susan Molinari?

MR. PRICE: No, Your Honor. It's Attachment 4.

THE COURT: No, no, no. I'm in your exhibit that you put in front of the Court. Right after Senator Blumenthal's letter, there is a page that says Attachment 2, letter from Susan Molinari. Received.

MR. PRICE: We do not need to introduce that into evidence.

THE COURT: Because it's not there, right?

MR. PRICE: I have not seen it.

THE COURT: Well, it's your exhibit. Then there is -- yes.

MR. SIMON: Judge, it's a part of our book, and it's what we've seen. And certainly if we're going to introduce the letter from the senators, we'd certainly want Google's statement to the Quartz article and the like.

THE COURT: All right. So there are four attachments, and you're not objecting that the exhibit goes in as presented because it will be the full exhibit. Is that correct, Mr. Simon?

MR. SIMON: Correct, Judge. Thank you.

THE COURT: It will be admitted, then.

(Defense Exhibit No. 53 is admitted into evidence.)

MR. PRICE: Thank you, Your Honor.

BY MR. PRICE:

Q I just want to turn to the body of the letter here because it seems to put Google on notice that Location History has some -- that the Senate had some concerns with Location History; is that correct?

A Just one point. Where this started was a walking away from the AP article which came out after this letter. This letter was sent on May 11. The AP

article was from August, I believe, later that year.
Q The Quartz article, I believe, preceded this and is cited in the letter --
A That's correct.
THE COURT: He's correct about the AP article; right?
MR. PRICE: Pardon me?
THE COURT: He's correct about the AP article.
BY MR. PRICE:
Q You are correct about the AP article.
A Okay. Because I just wanted to be clear. When you had previously asked me was I aware of additional scrutiny, I said yes. Then you referenced this letter, but this letter was written before that article.
So this letter was in response to the Quartz article, not the additional scrutiny that came as a result of the AP article.
Q Yes.
A Okay.
Q The letter criticized Google's Location History practices for -- this is 38 -- frequently mischaracterizing the service and degrades the functionality of products in order to push users into

providing permission, so says the letter.

Would you agree that's what it says?

A That's what it says in the letter, yes.

Q And the letter also says that these factors raise serious concerns -- raise serious questions about whether users are able to provide informed consent. Were you aware of that criticism, as well?

A That's what is in the letter, yes.

Q And I don't mean to be belabor this, but it does go on to say that Google's policies and explanations raise questions about their characterization of basic consumer protection terms, such as opt-in, opt-out, notice, consent, and anonymization according to the letter?

A That is what's in the letter, yes.

Q The letter calls the consent process confusing, 42?

A That is what's in the letter, yes.

Q And it cites Attachment 4. Attachment 4 -- is that correct? It cites Attachment 4?

A That's correct, yes.

Q And is this Attachment 4?

A I'm sorry. I didn't hear the question.

Q Is this Attachment 4?

A Yes, that is Attachment 4.

Q What does it show?
A This is one of the Google Assistant permission prompts.
Q And that includes Location History; correct?
A At that time it included Location History, yes.
Q The letter goes on to add that most consumers do not understand the level of granularity and reach of Google's data collection, and that there's serious questions about whether they have provided informed consent and maintain reasonable ability to avoid participating in this collection. Are you aware of that criticism, as well?
A That is what's in the letter, yes.
Q And the letter concludes by asking the FTC to open an investigation into the potential deceptive acts and practices used by Google to track and commoditize American consumers. Are you aware that the letter called for an investigation?
A I am aware that that is what's in the letter, yes.
Q So in addition to the news articles, and the Senate inquiry, Google got sued over Location History in 2018. Are you aware of that?
A Which particular case are you referring to?
Q The case is called *In re: Google, Location History Litigation*. It's a class action out of the

Northern District of California.

A Yes.

Q I'd like to show you Defense Exhibit 26. Is this the complaint in this case?

A Yes.

Q And you're aware of the complaint in the lawsuit?

A I am aware of this complaint, yes.

MR. PRICE: Your Honor, I would move to introduce the amended complaint for -- not for the truth of the matter, but for the fact that it exists.

THE COURT: Is there an objection?

MR. SIMON: Judge, I'd object to relevance. Obviously, it's hearsay through and through. But moreover, what we have, and the United States wouldn't object to things like the exhibit emails that are going to come from *Google v. Arizona* that shows communications between Google as a part of that litigation internal discussions. This is literally just some class action lawyer, presumably in California, that decided to go after Google.

The fact that it exists, the witness just admitted it. Putting it in the record, I think, does nothing more than continue sort of a broadside against Google more than just the article. This is just accusing Google of all kinds of things. And I don't

see any relevance to this being in the record.

THE COURT: These are just allegations. Why do we need to know -- has this class action completed?

MR. PRICE: It hasn't, Your Honor. The reason that we are talking about these things is because things like the newspaper articles, the congressional inquiries, and the lawsuits appear to have changed Google's behavior, changed Google's policies, and, in particular, have something to do with the relevant changes here to the Location History language.

So we're trying to establish what happened, what changed, why, and whether it was sufficient.

THE COURT: Well, I'm not going to admit this yet until you establish some fact that Google did that somehow you can say comports with something in the complaint. And even then, I'm not sure. These are just allegations. This is not -- this is not relevant to facts of what we need to consider in this case except that Google knew that the suit was ongoing and that it was about Location History.

So I'm going to sustain that objection.

MR. PRICE: Okay.

BY MR. PRICE:

Q Mr. McGriff, you're still aware of the lawsuit;

correct?

A I am aware of this lawsuit, yes.

Q It was filed just three days after that Associated Press story on August 17?

A I don't know how I would know.

Q It's right at the top of the page.

A If the date is there, then that's when it was filed, yes.

Q The main allegation here, and I don't mean to belabor this point either, is that Google "retains and continues to collect location data" --

THE COURT: Are you quoting from the complaint? Because I just said it's not admissible.

MR. PRICE: I'm not admitting it, Your Honor, I'm just trying to establish --

THE COURT: You're quoting it. You're admitting it by saying it.

MR. PRICE: Okay. I'll move on.

Your Honor, the allegations in this case, we understand that they are allegations.

THE COURT: What I said is, if you can show something that happened later that Google did that then you can show was alleged in this complaint, and there's some temporal proximity, then it is possible that this would be admissible. If you don't show yet

that there has been a change, no, it's not admissible.

MR. PRICE: Okay.

BY MR. PRICE:

Q There has been some discussion at Google since at least 2017 about changing the Location History language on the opt-in screen; is that correct?

A Are you referring to the consent or are you just referring to -- what language are you referring to specifically?

Q The language for opt-in to Location History through apps in particular or at setup where it says "Saves a private map of where you go." That language changed; correct?

A There has been discussion for the life of the product about what is the best copy to relay what the feature does, yes.

Q And you're aware that there are hundreds of pages of emails and documents that have been submitted to the Attorney General in Arizona discussing these sorts of changes?

A Yes, I am aware.

Q Specifically, on February 2, 2017, there's an email in which some Google engineers called Location History a mess. Does that sound familiar to you?

A I can't recall that specific copy, but if it's in

an email or document somewhere --

Q Perhaps I can refresh your recollection. Can I show you Defense Exhibit 36, please. It's up on your screen, as well.

A Just one clarification point. The screen has a black box on the side, so I can't see the text on the side, which is why I keep looking in the book.

I do see it on there as well, though.

Q I don't know how to --

A It's fine. I follow along with the book, but that's why I keep looking to the book and not the screen. It cuts it off.

Q Okay. So you can see there in the book?

A Yes.

Q And you can see that a little bit later on in that chain another Google employee described the location products as a "work in progress," and that Google was "trying to rein in the overall mess that we have with regards to data collection, consent, and storage"?

A That is what's mentioned in this, I guess, email exchange, yes.

Q And you have another Google employee who says, "How can we do a great job of respecting people's privacy when they don't want to share their location?"

A That is what's written in the exchange, yes.

Q And the same person says, "Can we have a foreground only model? Lots of users don't care about Location History."

A That is what's mentioned in the exchange, yes.

Q What's a foreground only model?

A I cannot even feign to understand what this person is referring to.

Q Does it refer to apps that are actively running as opposed to passively in the background?

A I believe what -- well, it's conflating several points. It's speaking to foreground only collection, which would be app specific, which is inherently not the nature of what Location History is or how its collection works. So this person is offering suggestions.

Q Okay. Thank you. A little bit later in that exchange, you can see at the bottom of your screen, it says -- there's another Google employee who wrote, "Do users with significant privacy concerns understand what data we are saving? Do they know how to control when we store location information?"

A That is a question asked in the exchange, yes.

Q And then, finally, you have a Google employee writing, "We have Location as a product umbrella that includes Location History and a bunch of other stuff

that's super messy. And it's a Critical User Journey to make sense out of this mess"?

A That is what's in the article or exchange, yes.

Q This is what Google employees were discussing in 2017 or is a recognition that there was a problem?

A There was some discussion about Location History, yes.

MR. PRICE: Sorry, Your Honor. Can I have one second?

THE COURT: Pardon me?

MR. PRICE: May I have one second?

THE COURT: Sure.

MR. PRICE: Your Honor, I would move to admit Defense Exhibit 36 into evidence, please.

THE COURT: Objection?

MR. SIMON: No objection, Judge.

THE COURT: Okay, it will be entered.

(Defense Exhibit No. 36 is admitted into evidence.)

BY MR. PRICE:

Q I'd like to turn your attention to Defense Exhibit 40. This is another February 2017 thread where a Googler says, "Personally, I can't think of a world where we do a good and thorough job with runtime permissions across Google apps that doesn't confuse

the hell out of our users." Are you aware of that email.

A I'm aware that that is a statement in this email, yes.

MR. SIMON: Judge --

MR. PRICE: I would like to move Defense Exhibit 40 into evidence, as well, Your Honor.

MR. SIMON: Judge --

THE COURT: Is there an objection?

MR. SIMON: Judge, I would only ask -- I'm not going to object to it being admitted, but a lot of these emails, including Defense Exhibit 40, has multiple pages, and I recognize that there's been prep here, but just to give the witness a second to look at the pages before pointing out the one sentence would be, I think, helpful.

THE COURT: That makes good sense.

So this is Defense 40, which is marked as Exhibit 236 in the first page. And I'm going to enter it into evidence.

And I will say, with your last set of questioning, you were going back and forth from one page to a page previous, and that was confusing. So I agree that you should be clear and certainly allow Mr. McGriff time to absorb it.

MR. PRICE: Thank you, Your Honor.

(Defendant's Exhibit No. 40 is admitted into evidence.)

Q This is page 5 of that PDF, of Exhibit 236.

THE COURT: I confused us by saying 236. It's 236 in the Arizona case. We should use our own exhibit numbers.

BY MR. PRICE:

Q So page 5 of Defense Exhibit 40.

MR. SIMON: Judge, I don't think we have exact page numbers. The bottom right of all of these *Google v. Arizona* emails what appears to be, like, a Bates stamp in their last five or three numbers, however you want to say it, but it looks like, you know, for this email it starts -- is this 236?

MR. PRICE: We can move on. I actually don't have any other questions about this chain.

THE COURT: Well, you just quoted something. Why don't you put on the record where you quoted it from. Something about "I can't imagine where," blah, blah, blah.

BY MR. PRICE:

Q This is the fifth physical page.

THE COURT: Look at the Bates number on the bottom right. You can also identify it by what the

first sentence is at the top of the page.

MS. KOENIG: It's not showing me the exhibit, Kathy.

THE CLERK: I think you must have turned it off.

MS. KOENIG: Let me unplug it and try it again. There we go.

BY MR. PRICE:

Q Do we have it here? So this is the page that is Bates stamp No. GOOG --

THE COURT: Just the last five digits.

MR. PRICE: 27381.

THE COURT: Thank you. And what did you place into the record?

MR. PRICE: I'll read it again. It says, "Personally, I can't think of a world where we do a good and thorough job with runtime permissions across Google apps that doesn't confuse the hell out of our users."

THE WITNESS: I don't think that's on that page.

THE COURT: No, it's not.

MR. PRICE: 27379.

THE COURT: All right. It's in the first full paragraph of 27379 that has a large redacted

block right before it, and it's sent, Monday, February 27, 2017, 23:37:44. All right. Now we know where you are.

MR. PRICE: Thank you for your patience.

BY MR. PRICE:

Q So, in addition to these 2017 emails, Google employees responded to the AP article in 2018, as well; correct?

A Is there a specific response you're speaking to or just generally that we were aware of the AP article?

Q Well, I'd like to show you Defense Exhibit No. 32. Do you have it?

A Yes, I do.

Q Great. So, you recognize this as an email chain in which Google employees are expressing concerns over the AP article?

A The entire exchange is redacted except for one section.

Q There's one section that's not redacted from August 13, 2018 at 9:38 a.m.

A That's correct.

Q And you recognize that as an email in response to the 2018 Associated Press article?

A That's correct, yes.

Q Okay. The email says that Google employees -- and

this is the page we're looking at here. It's page 4 of the PDF.

THE COURT: No, it is Bates No. 1523.

MR. PRICE: Bates No. 1523.

THE COURT: We do not have page numbers on the PDFs.

MR. PRICE: That is true.

BY MR. PRICE:

Q So on the page marked 1523, the email says that Google employees had what they called an "Oh Shit" meeting -- excuse my language, Your Honor -- meeting about the AP article; is that correct?

A It is my understanding that that is a regular meeting that that team has.

Q That's a regular meeting that the team has?

A That's correct. That's why it says "our Monday morning 'Oh Shit' meeting."

Q Good to know. It says, "Both comms and policy are looking for an update on where we are in terms of fixing Location History." Is that what it says?

A That is what it says, yes.

Q And Google prepared a PowerPoint of the impact of this AP article on Location History; is that correct?

A Is that an exhibit that I can --

MR. PRICE: Actually, I apologize, Your

Honor. Before we move on, I would like to introduce Defense Exhibit 32 into the record.

MR. SIMON: No objection, Judge.

THE COURT: All right. It will be moved into evidence.

(Defense Exhibit No. 32 is admitted into evidence.)

MR. PRICE: As well as Defense Exhibit 40.

MS. KOENIG: I'm sorry. We did that one.

MR. PRICE: We did that one. Okay.

THE COURT: 40 you're not objecting to?

MR. SIMON: Without objection, Judge.

THE COURT: It will be entered.

(Defense Exhibit No. 40 was admitted into evidence on page 244.)

BY MR. PRICE:

Q So Google prepared a PowerPoint presentation of the impact of the Associated Press article on the Location History product; is that correct?

A Are you referring to a specific PowerPoint?

Q I am. I'll bring it up as Defense Exhibit 33. It's from August 16, 2018.

A Yes, a PowerPoint was prepared for this incident as we would for any incident.

Q And we are on Bates No. 01458, Your Honor.

THE COURT: Uh-huh. Thank you.

BY MR. PRICE:

Q One slide here -- and this is 56, Laura -- shows a large jump in searches for -- that's Location History. It's Bates No. 01475.

THE COURT: 47 --

MR. PRICE: Five.

THE COURT: Five. Okay.

Q Are you aware?

A Yes, I'm aware that this slide quotes a spike here, yes.

Q It shows a very large increase in the number of search queries related to Google Location History; is that correct?

A That's correct.

MR. PRICE: I'd like to move Defense Exhibit 33 into evidence.

THE COURT: Any objection?

MR. SIMON: No objection.

THE COURT: It will be entered.

(Defense Exhibit No. 33 is admitted into evidence.)

BY MR. PRICE:

Q In fact, I don't know if this is surprising or was surprising to you, but Google has never actually

advertised Location History to its users; is that correct?

A Can you clarify what you mean by "advertise"?

Q Sure. I'll show you Defense Exhibit 34. Tell me when you have it.

A 34, yes.

MR. PRICE: Let us get the Bates stamp number for you, Your Honor, before proceeding. I do not believe -- so this does not have Bates stamps, but it is on page 37 of the actual document.

BY MR. PRICE:

Q Do you have it?

A Yes.

Q Okay. It says, As of today, we have not located online advertisements for Location History or Web & App Activity. If we locate any such responsive materials, we will promptly produce these representative examples.

So the question is whether Google has ever advertised Location History to its users?

A I see. So it's specifically referencing newspapers ads, magazines ads. In that context, no, we have not run any newspaper ads or magazine ads that I'm aware of, no.

Q Thank you.

MR. PRICE: Your Honor, I'd like to move Exhibit 34 into evidence as well.

THE COURT: Any objection?

MR. SIMON: No objection, Judge.

(Defense Exhibit No. 34 is admitted into evidence.)

BY MR. PRICE:

Q Referring to Location History settings, Google employees once again emailing, and this is Defense Exhibit 30, had some more to say about the Associated Press article. Can you go down? All right.

So this is page 7 of the actual PDF, and we'll get a Bates stamp number in a second. It is Bates 01271. Are you aware of these emails? These are from August 14, 2018.

A I see that these are emails, yes.

Q And they're referring to location settings. You have one Google employee here who writes, "It's a bit complicated, and we might need better messaging." Do you see that?

A That is what the message says, yes.

Q Are you aware of that?

A I see that now, yes.

Q And another Google employee wrote -- this is on Bates 01270. Another Google employee wrote, "I agree

with the article. Location off should mean location off; not except for this case or that case." Do you see that on the email?

A I see that that's what's written here.

THE COURT: Where is it?

MR. PRICE: This is Bates -- there you go.

THE COURT: I got it.

BY MR. PRICE:

Q And then it goes on to say, "The current UI" -- what's UI?

A User interface.

Q "The current UI feels like it is designed to make things possible, yet difficult enough that people won't figure it out. New exceptions, defaulted to on, silently appearing in settings menus you may never see."

So these are all responses to -- Google employees responding to the 2018 AP article; is that correct?

A These are people responding to the AP article, yes, that's correct.

Q Great.

MR. PRICE: Your Honor, I would like to introduce Defense Exhibit 30 into evidence, please.

MR. SIMON: Judge, I would ask to -- I would object to a fair amount of this coming in. So I

wouldn't object to 1266 through 1271, that top email on 1271, getting in, but if the Court looks through 1271 through 1287, it's a lot of talk about stuff that I don't think -- well, it's not relevant at all. The former President in is there, China restrictions in there, Elon Musk, a lot of stuff that should be redacted if the Court's going to allow this to be introduced.

I would note that I think Defense Exhibit 35 is a cleaner version of this. I could be wrong on that. But either way, I'd ask for the Court to admit it subject to the extraneous emails at the bottom starting on 1271 through 1287 being cut out.

MR. PRICE: I don't think we have a problem with that either. We have no intention of asking about Elon Musk or the former President.

THE COURT: All right. So the bottom half of 1271, which starts with "On Monday, August 13, 2018," blocked out entity "wrote," and the remainder of the exhibit will be excluded and not entered into evidence.

I agree that there seems to be some duplication in Exhibit 35.

MR. PRICE: Yes, Your Honor. These emails are duplicated in multiple places. The reason that we

chose to use this version of it was because it included the original formatting from those emails. So you're more able to see who's writing what, which people.

THE COURT: Okay. So the front part from 1266 to the top of 1271 and the cover page, which has no number, will be admitted. And the rest is excluded.

(Defense Exhibit No. 30 is admitted into evidence.)

BY MR. PRICE:

Q In fact, this email chain continues in Defense Exhibit 31, and it is not all contained in one exhibit. So I direct your attention, Mr. McGriff, to Defense Exhibit 31, which is the same thread of emails from August 14, 2018. And this is Bates 01289. Let me know when you have it.

A I have it, yes.

Q So one Google employee writes that it is "Definitely confusing from a user point of view if we need googlers explain it to us."

And a little bit further down. Is that correct? Sorry.

A That is what it says, yes.

Q And a little further down, user adds or an

employee adds -- this is Bates 01290. "Also seems like we are not very good at explaining this to users." Going on -- is that correct?

A That is what it says.

Q And then another Google -- the same Google employee writes, "Indeed we aren't very good at explaining this to users. Add me to the list of Googlers who didn't understand how this worked and was surprised when I read the article."

A That is what was written there, yes.

Q So these are Google employees who are reading this article and are surprised to learn how Google's location settings actually work?

A I would frame it as this is a group of Googlers commenting on the interaction of Google settings, yes.

Q That same employee goes on to say, "Of course, we shouldn't have to explain this to users. The real failure is that we shipped a UI that confuses users and requires explanation"; correct?

A That is what it says, yes.

Q And that person goes on to suggest that "We should redesign the UI so it's obvious what's happening, and make it easy for users to choose the settings they want in one place without parsing complex details about product interactions." Is that what it says?

A Yes. I have no idea what UI they are talking about, but that is what it says.

Q And there's only one more thing that we can read on this chain. One more user just wrote, "Please don't comment!"

A That is what is written, yes.

Q So from these emails -- excuse me one second.

MR. PRICE: Your Honor, I would like to move to admit Defense Exhibit 31, please.

THE COURT: Objection?

MR. SIMON: Judge, subject to the same objection, there's a lot of extraneous talk. I think it's at all extraneous between 1293 and 1309. So we wouldn't object to admitting it but cutting out those pages.

MR. PRICE: That's acceptable to us, as well.

THE COURT: All right. It will be admitted through 1292, and not 1293 through 1309. I have an extraneous document in here, I think. It looks to be a LexisNexis search. Does somebody have that at the end?

MS. KOENIG: It was probably my putting this together too hastily, Your Honor.

THE COURT: All right. Well, to the extent it just looks as if somebody looked up a particular

case, it seems unrelated. So that will not be admitted either.

MR. PRICE: Thank you, Your Honor.

(Defense Exhibit No. 31 is admitted into evidence.)

BY MR. PRICE:

Q Okay. So following the AP story, following -- the Google employees wrote to each other about this issue over Location History; correct?

A Employees discussed the article, yes.

Q And then Google changed its privacy policy -- correct? -- in May of 2018?

A The privacy policy?

Q Uh-huh. On May 25, 2018, Google issued an update to its main privacy policy. Are you aware of that?

A I don't recall that.

Q Perhaps I can refresh your memory.

MR. PRICE: Can we see Defense Exhibit 43, please.

Q I'm showing you a redline version of the policy when it was enacted on May 25.

A Okay. Sorry. This is not -- okay, yes. There was a privacy policy update in May, yes.

Q And this is the privacy policy that was updated?

A Yes, this is a privacy policy update from

May 2018.

Q Okay. And the previous one had --

A But -- sorry. I guess why I'm confused, this privacy policy that you're referring to here was before the AP article.

Q I'm sorry. It was a change before the AP article after the Senate inquiry and after the Quartz article; is that correct?

A I'm sorry. There was -- the -- I think these things are orthogonal. The privacy policy was updated full stop independent of inbound letters specifically from senators about Location History.

Q I'm not saying that -- I'm not asking you if one caused the other. I'm just asking if this was the privacy policy --

THE COURT: Well, you sort of are. You're saying after the AP article, Google updated its privacy policy. So you're suggesting there is a relationship. So let him answer the way he wants to answer.

A Yeah. These are orthogonal events. There are many moving pieces happening all the time. I assure you, there's no way Google updated its privacy policy in two weeks. If the Senate letters were May 11, this is May 25. So this privacy policy update must have

been well in flight well before those letters were received, which would not be related to the AP article or the communication in that group digest about response to the AP article.

So I guess that's why I'm just saying they're orthogonal. There are a series of things that happened in the arc of everyone is always making further improvements, yes.

Q And Google had been talking about making changes for quite some time to this language going back to at least 2017, as we discussed earlier; correct?

A In the privacy policy?

Q The Location History language.

A For the life of the product we have -- every Google product we are always looking for ways that we can provide further transparency and clarity.

Q Does the feedback that you receive either in the press or from members of Congress impact those discussions?

A I think all feedback informs those discussions on a regular basis, yes.

Q All right. Great. This privacy policy change happened on May 25, 2018; is that correct?

A That's correct, yes.

Q Okay. And you recognize this privacy policy

change?
A I have not looked at this in some time. Is there a specific section?
Q Yes, I just want to admit this. So I would like to know if you recognize this as Google's privacy policy from May 25, 2018?
A I could not certify that this is the privacy policy as it stood on May 25, 2018. It does appear to be some iteration of the privacy policy at some point, but that was several years ago now.
Q It says that the -- if you go back up to the top --
THE COURT: Is there objection to him using this at the very least as a demonstrative exhibit? I mean, this is essentially how this witness has identified most of these exhibits. It's not being offered for the truth of the matter. It says it's May 25. It's a redline version. Can we at least treat it on that basis?
MR. SIMON: Yes, Judge. Yes.
THE COURT: Okay. So it's admitted on that limited basis.
MR. PRICE: Thank you, Your Honor.
(Defense Exhibit No. 43 is admitted into evidence.)

Q It says that the previous policy had been in effect since December 18, 2017, right up at the top there.

THE COURT: You really have to --

MR. PRICE: Sorry.

BY MR. PRICE:

Q I'm at the first page at the very beginning where it says "last modified," right underneath "privacy policy." There's December 18, 2017 crossed out, and the next date there that's not crossed out is May 25.

A Oh, I see. That is the crossed out date. This shows that this was an update after the December 18, 2017 update, yes, that's correct.

Q Are you aware that the previous policy, the one that was in effect until December 18, 2017, did not mention Location History whatsoever?

A I was not aware of that, no.

Q Were you aware that this is the first version that mentions Location History by name?

A Can you point me to the context where this introduces Location History?

Q Yes. We are on page -- it was 7 of the PDF itself. It doesn't come with its internal page numbers.

THE COURT: So just say what headings are on

it so we can look through the document quickly.

BY MR. PRICE:

Q It's under the heading "Your location information." I'm at the bottom of the page that contains that heading.

A I would have to check to confirm, but that does not ring correct to me, because we do have -- on the location policies page, there is a mention and has been a mention of Location History. We did make an update to that page to further refine the language around Location History in 20- -- either later 2018 or early 2019, but that was a refinement to existing copy, not the introduction of.

In this particular draft where you have redactions, is there a suggestion that all of this content is new?

Q There shouldn't be any redactions --

A Sorry. Not redactions. I meant the crossed out copy.

Q This is Google's redline. It's available on their website. The crossed out language is the old language, and the language that isn't crossed out is the new language.

THE COURT: Okay. I'm still not with you, unfortunately. So what part of the page is your

Location History on? Is it your --

MR. PRICE: "Your location information."

THE COURT: All right. Now I'm with you.

BY MR. PRICE:

Q Just to clarify, I'm asking about the privacy policy that we're looking at, not the help pages.

A I understand. And this might just be my misunderstanding of how it's structured or maybe how it's labeled externally, but we do have on the broader company policy's page under "technologies," there's a whole section about location usage. That copy was refined, but it existed, which is why I'm surprised. I would need to check.

Q The copy that you're describing, is that the same as the privacy policy or is that that something different?

A There's a broader privacy policy that has sections, and one of those sections is like a subsection. It's, like, policies.google.com/location or technologies/location, something like that. And there exists a description of the location copy. That was refined in this time period. It wasn't introduced.

Q The technologies page and the copy that is there is not included in the privacy policy itself?

A I believe it is a part of the privacy policy because I think you have to go to the privacy -- I'd have to check. I don't know.

THE COURT: He's not giving you the answer you want. He's not able to say that this is the first time it ever appeared. What he has just testified is that there is some kind of web policy that he is aware of, and he just said, I would be surprised if this were the first time it were in the privacy policy because I'm aware that we had it in a bigger website policy that had been refined.

So you just didn't get the answer you wanted, even though you're going to argue that because it doesn't have strike-throughs, this was the first time it came in. He's given you the answer he has.

MR. PRICE: Thank you, Your Honor. We will move on.

BY MR. PRICE:

Q Google changed the opt-in language for Location History in 2018; correct?

A By opt-in language, do you mean the consent?

Q Yes.

A The Location History consent itself has not changed.

Q The language in the consent flow didn't change at

all during 2018?

A The consent flow is not the consent. The actual Location History consent has not changed.

Q I'm speaking about the consent flow --

THE COURT: Why don't you show an example.

MR. PRICE: Laura, can we pull up Mr. McInvaille's report.

BY MR. PRICE:

Q Let me turn your attention to Defense Exhibit 7.

MR. PRICE: Can you go up a little bit, Laura?

BY MR. PRICE:

Q So we see a screenshot here from early in 2018. The language under Location History says "creates a private map of where you go with your signed in devices."

A That's what is it says, yes.

Q Right. And can we go to the next figure, please. This is a screenshot provided by Oracle, also in early 2018. And it says "creates a private map of where you go with your signed-in devices."

A That is what it says.

Q Right underneath Location History.

Can we look at the third one from the Norwegian Consumer Council from July 2nd of 2018? And in the

middle screenshot underneath Location History, it says, "Saves where you go with your devices."

A That is what it says, yes.

Q So that language is different from the previous two screenshots that we just discussed?

A That is not the Location History consent copy, which is in the expanded block in the third exhibit you reference, but the descriptive copy did change, yes.

Q And that changed in 2018; is that correct?

A That changed as a result of GDPR, yes.

Q Do you know when it 2018 it changed?

A When was -- I couldn't say exactly.

THE COURT: As a result of what? I'm sorry, sir.

THE WITNESS: Sorry. One of the requirements of GDPR was that we be able to centrally serve all strings from a single data store. So part of our compliance with that policy was to standardize all of these strings because they were leading from the same store. That work was in flight in 2018.

So depending on when the screenshots were taken, you might see some slight variations as you just pointed out in these two screens for the descriptive copy itself, yes.

THE COURT: All right. So GDPR?

THE WITNESS: That's the General Data Protection Regulation.

THE COURT: Thank you.

BY MR. PRICE:

Q That was a new law enacted in Europe governing the privacy rights of individuals and their data?

A That is correct, yes.

Q So -- but Google had been discussing the need to change this particular language for quite some time; correct?

A No.

Q No? You're not aware of the emails discussing the need to change the "creates a private map" language?

A Sorry. I think some things are being conflated. Which emails are you referring to?

Q These are part of the *Arizona v. Google* emails, the emails that Google turned over to the Arizona Attorney General.

A If I recall -- I would need to see the exchange, because if I recall the exchange you're referring to, it's referring to a different set of disclosures that we were working to align our presentation, but is there an example here?

Q Sure.

MR. PRICE: Can we show Defense Exhibit 41, please? And this is Bates 57339.

MR. DUFFEY: 379?

MR. PRICE: 57339.

A I see it, but to my previous point, this exchange is referring to a different string of copy. It's not referring to the -- what's being discussed at the bottom is not related to the "creates a private map." The "creates a private map" in quotes there is like the language was just like a flag of the page where this language appears, but this exchange specifically was in reference to the conflation with WAA that was discussed, which is why it was relevant in the Arizona matter.

Q When did this copy appear that's being discussed?

A There's that descriptive string that says "saves a map of the places where you go with your signed-in devices" or "creates a private map." That is not what we were discussing here. This exchange at the bottom is specifically referring to -- yeah, this was broader. I guess, maybe I'm not following the connection.

Q Well, the consent flow, at least the initial screen with the one-line description, changed sometime in 2018. It used to say "creates a private map," and

it doesn't anymore. This email exchange appears to be talking about whether to change the "creates a private map" language, which a Google employee describes as one of the most admired pieces of prose in the privacy space at Google.

A Okay. I'm just not following. I apologize. This language is referring -- so, the exchange here is referring very broadly to the descriptive copy, yes. Maybe I'm missing the point. Sorry. What's the question for me?

Q It says that Google had a long, mostly political, fight over the private map language. I apologize. It's on the next page.

THE COURT: 340?

MR. PRICE: Yes, Your Honor, in the middle of the page.

A I'm sorry. That is what it says, yes.

Q And you don't recall what this is in reference to?

A No. It says what it's in reference to. This is in reference to the descriptive copy. It's not related to the Location History consent copy at all. It's how exactly it's framed. And this discussion is in the context of the alignment of all the copy because we were going to consolidate and all read from the same central store.

Q So you're saying there was secondary copy, that second screen that you're talking about, that contained this language at some point?

A No. There's the LH consent copy, which has been static. That has not changed. And then there was descriptive copy that would appear in a snippet either immediately before, and then there's also immediately after.

In that time period, we were looking at refining and aligning the descriptive copy strings because prior to that point, they were all baked into the native apps.

So if you had to make a change, for example, on IOS, you had to submit an update to the app store. If you had to make a change on Android, you had to publish a new APK. We had to do it manually.

Part of what we were doing in 2018 was aligning so that these were all readable from some single store. And they weren't baked into the app. Instead the app was just calling to say what string should I show in this WAA.

So there was lot of discussion around how can we further refine all of those strings to make them consistent with each other in terms of their framing. This exchange is specifically referencing, it sounds

like, several of the different controls. So, yes, several of the different controls and balancing the pros and cons of different options.

They don't speak specifically to the consents because the consents weren't being changed. It's just simply to the descriptive copy around the consents.

Q So this is talking about a change to the descriptive copy? That one line underneath where it says Location History.

A The exchange is speaking to the descriptive copy around the consent, that's correct.

Q And one employee actually goes on to say, "My preference is 'Saves where you go with this device'"; correct?

A Yes, I see that here.

Q And that is very, very similar to what the first screen in the Location History consent flow, the descriptive screen, ends up being changed to; correct?

A That is correct, yes.

Q So was it a coincidence?

A So, this is from 2017, January. So coincidence with what?

Q That -- you're saying that this discussion is not referencing a change to the Location History description during the consent flow process.

A I apologize. Maybe I'm getting confused. There are always discussions in flight around how we can further improve our products and services and further clarify.

This discussion from 2017 is about changes that might be suggested to, it looks like, various controls, including Location History, to further improve transparency around them. So that is that.

So, yes, it is a discussion across several controls over further improvements that can be made to their descriptive copy, yes. And then you're linking this to the 2018 update? To the Location History page?

Q No, I'm saying --

THE COURT: Exhibit 17, are you comparing it back to Exhibit 17? That's his question. You showed him Exhibit 17 -- Exhibit 7, your expert's report. Is that what you're trying to carry it back to?

MR. PRICE: Excuse me? We're talking about the -- I'm sorry.

THE COURT: The descriptive text on Exhibit 7 under Location History from 7-2-2018, which is how you began this process, says "saves where you go with your devices." Is that the link you're trying to make?

MR. PRICE: Yes. I'm asking if the

discussion here had to do with the language that we see in this language change that eventually happened in 2018.

BY MR. PRICE:

Q My question for you initially was, a discussion about this language had been in the works for quite some time, since at least 2017.

A I see. So this is why -- I don't think you can flatten it in the way that you're attempting to, because of the screenshots being from a point in time. For example, I could leave this courtroom right now and go to a Best Buy and buy a device that's three years old and take it off the shelf and take screenshots. The images that I see would be taken today but be a reflection of what was baked into that device when it was shipped to the shelf three years ago.

So the screenshots here, the date of the screenshots is not sequential in terms of when we release the copy updates. So the language decisions being discussed here in your Exhibit 41 around "saves a map," those were likely introduced into production shortly after. It is highly probable that -- especially because these are from a series of different sources with very different narratives and

very different agendas.

Oracle is going to find the least favorable example. And so they'll use a screenshot that's beneficial to them. In a research study, they might just choose to benchmark when they're looking across several different sources. And they'll take screenshots that were beneficial to them.

So from the screenshots alone, I can't say -- and you can correct me if I'm wrong -- I can't say that this change was before that change or was tied to the Exhibit 41 discussion.

Based on reading these exchanges, this 2017 discussion was baked and put into prod, and at some point percolate into -- I'm sorry. Into production. And at some point percolated into product. These screenshots are just at different points in time in the life of the product.

So that is how you see the evolution here is not directly tied to the previous things we've been discussing, like the AP article or other changes that were happening in 2018.

THE COURT: All right. We're done. So it is 10 minutes almost after when I said I have to leave because I have a conference call that is an emergency. And so I apologize for the abrupt ending, but we'll

continue this tomorrow.

And, sir, you will still be under oath. You can't discuss your testimony with anyone. That will give us time. Maybe all of us will be a little more clearheaded about what relates to what, not at 5 o'clock in the evening. And we'll pick up from there. So the cross will continue.

I'm going to remind everybody to make sure that your witnesses are sequestered. Can we start tomorrow at nine?

MR. PRICE: Yes, Your Honor.

MR. SIMON: Yes, Your Honor.

MR. GILL: That's fine, Judge.

THE COURT: All right. So we will begin tomorrow at nine. And if folks want to call in, they may do so then.

Is there anything else I need to cover?

MR. SIMON: Nothing further, Judge.

MR. PRICE: Nothing further. Thank you, Your Honor.

THE COURT: Okay. My apologies for this call happening, but I have no control.

(The proceedings were adjourned at 4:55 p.m.)

I, Diane J. Daffron, certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/s/

_____ _____

DIANE J. DAFFRON, RPR, CCR DATE

This page intentionally left blank for double-sided pagination and printing

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Richmond Division (The Hon. M. Hannah Lauck)

JOINT APPENDIX

VOLUME 4 of 11 (pages 695 - 1070)

JESSICA D. ABER
United States Attorney

Kenneth R. Simon, Jr., Ass't U.S. Attorney
Peter S. Duffey, Ass't U.S. Attorney
Counsel for Appellee
919 East Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400

Nathan P. Judish, Senior Counsel
Computer Crime & Intel. Property Section
Criminal Division
U.S. Department of Justice

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
Counsel for Appellant
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800

Michael W. Price, Litigation Dir.
NACDL Fourth Amendment Ctr.
1660 L Street NW, 12th Floor
Washington, DC 20036

This page intentionally left blank for double-sided pagination and printing

TABLE OF CONTENTS

VOLUME 1 (pages 1 - 176)

District Court Docket Sheet (as of Jan. 17, 2023) 1

Indictment (Sept. 17, 2019, Doc. 1) 22

Defendant's Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Oct. 29, 2019, Doc. 29) 25

Government's Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (Nov. 19, 2019, Doc. 41) 51

Defendant's Reply to Government's Response [to] Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Dec. 9, 2019, Doc. 48) 76

Exh. A (First Step 2 Request to Google) (Doc. 48-1) 98
Exh. B (Second Step 2 Request to Google) (Doc. 48-2) 100
Exh. C (Third Step 2 Request to Google) (Doc. 48-3) 102
Exh. D (Transcript, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019)) (Doc. 48-4) ..... omitted from J.A.

Government's Notice Regarding Attachment of Google Geofence State Search Warrant to Response in Opposition to Motion to Suppress (Dec. 18, 2019, Doc. 54) 104

Affidavit for search warrant and warrant, with attachments (Doc. 54-1) 107

Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant (Dec. 20, 2019, Doc. 59-1) 118

United States' Response to Amicus Curiae Brief of Google LLC (Jan. 10, 2020, Doc. 71) 148

Defendant's Response to Google's Motion to File Amicus Curiae Brief in Support of Neither Party (Jan. 10, 2020, Doc. 72) 158

VOLUME 2 (pages 177 - 416)

Transcript, Discovery Motion Hearing (Jan. 21, 2020, Doc. 81; *see* Doc. 77 (court minutes))....177

Preliminary matters....179

Def't witness Spencer McInvaille — Direct examination....193; Cross examination....283; Redirect examination....306

Argument by the defense....318
Argument by the government....332
Rebuttal by the defense....350

Court's ruling....355

Defendant's Supplemental Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (May 22, 2020, Doc. 104)....363

United States' Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (June 12, 2020, Doc. 109)....393

VOLUME 3 (pages 417 - 694)

Transcript, Suppression Motion Hearing, Day 1 (evidence) (Mar. 4, 2021, Doc. 201; *see* Doc. 198 (court minutes))....417

Preliminary matters....420

Def't witness Spencer McInvaille — Direct examination....432; Cross examination....542; Redirect examination....586

Def't witness Marlo McGriff — Direct examination....606

VOLUME 4 (pages 695 - 1070)

Transcript, Suppression Motion Hearing, Day 2 (evidence) (Mar. 5, 2021, Doc. 202; *see* Doc. 199 (court minutes)) 695

Preliminary matters 698

Def't witness Marlo McGriff, cont'd — Direct examination ..... 699; Cross examination ..... 791; Redirect examination 841

Def't witness Sarah Rodriguez — Direct examination ..... 862; Cross examination ..... 902; Redirect examination 916

Gov't witness Jeremy D'Errico — Direct examination ..... 923; Cross examination ..... 967; Redirect examination 1010

Gov't witness Joshua Hylton — Direct examination ..... 1016; Cross examination ..... 1040; Redirect examination 1063

Concluding matters 1064

VOLUME 5 (pages 1071 - 1326)

Defendant's Post-Hearing Brief on "Geofence" General Warrant (May 3, 2021, Doc. 205) 1071

Government's Response in Opposition to Defendant's Motion for Suppression (May 21, 2020, Doc. 214; *see* Doc. 207-2) 1117

Defendant's Reply to Government's Response in Opposition to Motion for Suppression (June 4, 2020, Doc. 213) 1164

Transcript, Suppression Hearing (arguments) (June 24, 2021, Doc. 217; *see* Doc. 215 (court minutes)) 1185

Argument by the defense 1187
Argument by the government 1231
Rebuttal by the defense 1313

Concluding matters 1322

VOLUME 6 (pages 1327 - 1456)

Memorandum Opinion (denying suppression motion) (Mar. 3, 2022, Doc. 220) 1327

Order (denying suppression motion) (Mar. 3, 2022, Doc. 221) 1390

Criminal Information (May 6, 2022, Doc. 224) 1391

Transcript, Change of Plea Hearing (May 9, 2022, Doc. 247; *see* Doc. 226) 1394

Plea Agreement (May 9, 2022, Doc. 228) 1428

Statement of Facts (May 9, 2022, Doc. 229) 1444

Judgment in a Criminal Case (Aug. 19, 2022, Doc. 239) 1449

Notice of Appeal (Aug. 25, 2022, Doc. 241) 1456

VOLUME 7 (pages 1457 - 1810) – DOCUMENT EXHIBITS

Exhibits Admitted at Discovery Motion Hearing (Jan. 21, 2020)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) ..... *see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) ..... *see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) ..... *see* J.A. 2093
Def't Exh. 4: Activation Video ..... omitted from J.A., available on request
Def't Exh. 5: Three Paths Video (sealed) ..... *see* J.A. 2139
Def't Exh. 6: First Step 2 Request to Google 1457
Def't Exh. 7: Second Step 2 Request to Google 1459
Def't Exh. 8: Third Step 2 Request to Google 1461

Def't Exh. 9: Step 3 Request to Google 1463

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) .....*see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) .....*see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) .....*see* J.A. 2093
Def't Exh. 5: Three Paths Video (sealed) .....*see* J.A. 2139
Def't Exh. 6: Spencer McInvaille Report 1464
Def't Exh. 7: Spencer McInvaille Supplemental Report 1469
Def't Exh. 8: CSV Google Data File (.csv file) .....*see* J.A. 2139
Def't Exh. 9: Unique in Crowd Study 1475
Def't Exh. 11: September 2018 Oracle Submission 1480
Def't Exh. 18: Federal Search Warrant Application & Attachments 1502
Def't Exh. 19: State Search Warrants & Attachments 1534
Def't Exh. 21: McGriff Declaration 1 (Doc. 96-1) 1551
Def't Exh. 23: McGriff Declaration 3 (Doc. 147) 1562
Def't Exh. 24: Rodriguez Declaration (Doc. 96-2) 1579
Def't Exh. 27: Every Step You Take 1587
Def't Exh. 30: AZ Ex. 18 (admitted portions only) 1631
Def't Exh. 31: AZ Ex. 19 (admitted portions only) 1633
Def't Exh. 32: AZ Ex. 20 1639
Def't Exh. 33: AZ Ex. 24 1644
Def't Exh. 34: AZ Ex. 202 1667
Def't Exh. 36: AZ Ex. 209 1777
Def't Exh. 38: AZ Ex. 219 1781
Def't Exh. 40: AZ Ex. 236 1797
Def't Exh. 41: AZ Ex. 260 1804

VOLUME 8 (pages 1811 - 2090) – DOCUMENT EXHIBITS, CONT'D

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021), cont'd

Def't Exh. 43: May 2018 Privacy Policy – Redline 1811
Def't Exh. 43a: May 2018 Privacy Policy – Redline (with internet source information) 1840
Def't Exh. 44: Jan. 2019 Privacy Policy – Redline 1865
Def't Exh. 45: Oct. 2019 Privacy Policy – Redline 1895
Def't Exh. 46: McGriff Blog 1 1926

Def't Exh. 47: McGriff Blog 2 1929
Def't Exh. 48: 2018 Quartz Article 1934
Def't Exh. 49: 2018 AP Article 1 1941
Def't Exh. 51: 2019 NYT Article 1948
Def't Exh. 53: Blumenthal-Markey Letter to FTC 1957

Gov't Exh. 1: CAST PowerPoint Presentation 1981
Gov't Exh. 2: Geofence Warrant (Doc. 54-1) ..... *see* J.A. 107
Gov't Exh. 3: Declaration of Marlo McGriff (Mar. 11, 2020)
(same as Def't Exh. 21 (Doc. 96-1)) ..... *see* J.A. 1551
Gov't Exh. 3a: Declaration of Sarah Rodriguez (Mar. 11, 2020)
(same as Def't Exh. 24 (Doc. 96-2)) ..... *see* J.A. 1579
Gov't Exh. 3b: Supplemental Declaration of McGriff (June 17, 2020)
(Doc. 110-1) 2032
Gov't Exh. 3c: Third Declaration of Marlo McGriff (Aug. 7, 2020)
(same as Def't Exh. 23 (Doc. 147)) ..... *see* J.A. 1562
Gov't Exh. 4: Joshua Hylton emails with Google 2034
Gov't Exh. 5: Google Privacy Policy 2048
Gov't Exh. 5a: Google Terms of Service 2081
Gov't Exh. 6: Special Agent D'Errico's C.V. 2088
Gov't Exh. 12: "Got to Be Mobile" Video ..... *see* J.A. 2091

VOLUME 9 (pages 2091 - 2092) – DIGITAL MEDIA EXHIBIT

Gov't Exh. 12: "Got to Be Mobile" Video (admitted only at suppression motion hearing) ..... (.mp4 file)

VOLUME 10 (pages 2093 - 2138) – SEALED DOCUMENT EXHIBIT

Def't Exh. 3: PDF of Raw Data (*see* Doc. 69 (sealing order)) (admitted at both discovery motion hearing and suppression motion hearing) 2093

VOLUME 11 (pages 2139 - end) – SEALED DIGITAL MEDIA EXHIBITS

Def't Exh. 5: Three Paths Video (admitted at both discovery motion hearing and suppression motion hearing) ..... (.mp4 file)
Def't Exh. 8: CSV Google Data File (admitted only at suppression motion hearing) ..... (.csv file, viewable in Excel)

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA	
v.	Criminal No. 3:19CR130
OKELLO T. CHATRIE	March 5, 2021

DAY TWO

COMPLETE TRANSCRIPT OF MOTION TO SUPPRESS
BEFORE THE HONORABLE M. HANNAH LAUCK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

Kenneth R. Simon, Jr., Assistant U.S. Attorney
Peter S. Duffey, Assistant U.S. Attorney
U.S. Attorney's Office
SunTrust Building
919 East Main Street, Suite 1900
Richmond, Virginia 23219

Nathan P. Judish, Assistant U.S. Attorney
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, Virginia 20530

Counsel for the United States

Laura J. Koenig, Assistant Federal Public Defender
Paul G. Gill, Assistant Federal Public Defender
Office of the Federal Public Defender
701 E. Broad Street, Suite 3600
Richmond, Virginia 23219

Counsel for the Defendant

DIANE J. DAFFRON, RPR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT

APPEARANCES: (Cont'd)

Michael W. Price, Esquire
National Association of Criminal Defense Lawyers
1660 L Street, NW
12th Floor
Washington, DC 20036

Counsel for the Defendant

I N D E X

	DIRECT	CROSS	REDIRECT
MARLO McGRIFF	282	374	424
SARAH RODRIGUEZ	445	485	499
JEREMY D'ERRICO	506	550	593
JOSHUA HYLTON	599	623	646

E X H I B I T S

DEFENDANT'S EXHIBITS:		Page
No. 18	Federal Search Warrant Application	636
No. 19	State Search Warrants & Application	632
No. 24	Rodriguez Declaration	449
No. 41	AZ Ex. 260	283
No. 43A	Privacy Policy - Redline	301
No. 44	Jan. 2019 Privacy Policy - Redline	302
No. 45	Oct. 2019 Privacy Policy - Redline	322
No. 51	2019 NYT Article	303

GOVERNMENT'S EXHIBITS:

		Page
No. 1	CAST PowerPoint Presentation	515
No. 2	Geofence Warrant	522
No. 3	Declaration of Marlo McGriff	375
No. 3A	Declaration of Sarah Rodriguez	486
No. 3B	Supplemental Declaration of McGriff	375
No. 3C	Third Declaration of Marlo McGriff	375
No. 4	Joshua Hylton Emails with Google	621
No. 5	Google Privacy Policy	386
No. 5A	Google Terms of Service	386
No. 6	Special Agent D'Errico's C.V.	511
No. 12	Video	395

(The proceedings in this matter recommenced at 9:05 a.m.)

THE CLERK: Day two. Case No. 3:19CR130, United States of America versus Okello Chatrie.

The United States is represented by Kenneth Simon, Peter Duffey, and Nathan Judish. The defendant is represented by Laura Koenig, Michael Price, and Paul Gill.

Are counsel ready to proceed?

MR. SIMON: The United States is ready, Your Honor.

MS. KOENIG: The defense is ready, Your Honor. Good morning.

THE COURT: All right. Well, welcome back. We have folks on AT&T. So I just need to remind our individuals who are joining us by conference call through AT&T that we have a local rule, Criminal Rule 53, and a standing order that prohibits the separate recording or transmission or broadcast of this hearing. We have our court reporter here making our official court record, and there will be no other record made in the case.

So thank you all again. We're all ready to go. I see that Mr. McGriff is on the stand.

And, Mr. McGriff, I have to remind you that

you're still under oath. And we will continue where we left off yesterday. Thank you all very much.

MR. PRICE: Thank you, Your Honor. Good morning.

THE COURT: Good morning.

BY MR. PRICE:

Q Good morning, Mr. McGriff.

A Good morning.

Q How are you?

A Doing well. How are you?

Q I'd like to start with just a bit of housekeeping from the end of the day yesterday. We were talking about Defense Exhibit 41, which is an email chain from January 28, 2017, in which Google employees are discussing the language used to describe Location History. Do you recognize that email?

A Yes, this is the email from yesterday.

MR. PRICE: I would just move to admit this into evidence, Your Honor.

THE COURT: Is there any objection?

MR. SIMON: No objection, Judge.

MR. PRICE: Thank you.

BY MR. PRICE:

Q Now, yesterday you --

THE COURT: I'm just going to say on the

record that it's entered. We all know it is, but I hadn't gotten to that page of your exhibit list yet. Pardon me.

(Defense Exhibit No. 41 is admitted into evidence.)

BY MR. PRICE:

Q Yesterday you testified that you didn't know the precise number of users with Location History enabled in 2019?

A No, I do not know that precise number.

Q But you did say in your affidavit that roughly a third of active users had Location History enabled in 2019?

A Active Google accounts, yes.

Q And that that amounted to numerous tens of millions of Google users. Could you walk us through how you got to that figure, one-third and numerous tens of millions?

A At the time that that was being prepared, we looked at the total number of users who had Location History enabled for their account. That figure was prepared over a year ago. I believe we also looked at the number of active Google accounts. And then I believe we also looked at, for Location History specifically, whether or not the account was active.

Q Okay. Do you recall what the whole number with Location History enabled was?
A I don't recall the whole numbers. Again, we prepared those, at this point, well over a year ago.
Q So you came out with the figure of one-third. How did you figure out the denominator?
A We looked at the total number of Google accounts as provided by that team, and we asked at the time for the life of the product. The number has always roughly been a third. And so when we were preparing the -- I believe it was the first brief, and then also my first declaration, we verified all the numbers again, and it was still roughly a third.
Q But you have no recollection of what that number was?
A I could not recall that number off the top of my head. I'm sorry.
Q So within 50 million?
A I do not recall that number off the top of my head. I'm sorry.
Q All right. Shift gears a little bit. I want to call your attention to your third exhibit or your third declaration, which is Exhibit 23, the second page, in which you say Google's records reflect that Okello opted in to the Location History service on

July 9, 2018; is that correct?
A That is what it says, yes.
Q At 4:09 UTC?
A That is what it says, yes.
Q And Location Reporting was enabled at the same time?
A That is correct, yes.
Q And that can only happen, according to your declaration, when the opt-in occurs through a device based consent flow?
A That is correct.
Q In other words, you can't -- you can say you're sure it happened on the phone and not on a browser on a desktop?
A That's correct, yes. Excuse me. Just to clarify. That it happened on that specific device, yes.
Q Thank you. On the third page, you say that you, as in Google, does not have a record of the specific interface, i.e., the particular application or setting opt-in screen that Mr. Chatrie used to enable Location History; is that correct?
A That is correct, yes.
Q But as of July 9, 2018, it was possible to opt in to Location History when attempting to use a feature powered by Location History. That's what you wrote?

A That is correct, yes.
Q And it's true?
A That is true, yes.
Q An example would be the Google Maps application?
A That is correct, yes.
Q Another example would be the Google Photos application?
A That is correct, yes.
Q And another example would be the Google Assistant application?
A At that time we were removing the opt-in through Assistant. I think one of the things we were looking into was it still possible on that exact date, but there was support roughly in that time period to opt in to Location History through Assistant, yes.
Q You don't mention Google Assistant in your application, do you, or in your declaration?
A In my application --
Q Your declaration, sorry.
A In my declaration, I don't believe I mentioned an exhaustive list of opt-ins.
Q Okay. And just to be clear, Location History could have been enabled here through the Google Assistant setup?
A That is possible, yes.

Q Okay. The defense has an expert opinion saying that based on a forensic examination of the phone, Location History was enabled through the Google Assistant app, which was installed at virtually the same time. You don't have any information to dispute that, do you?

A I do not, no.

Q All right. So with that in mind, I want to go back and try and clear up a little bit of confusion from yesterday. You said that you didn't remember if Google had changed its privacy policy on May 25, 2018; is that correct?

A I did not -- I do not recall any location specific changes in the privacy policy in May 2018, that is correct.

Q Okay. Now, if you were to look at a list of Google's past privacy policies and see those redlines, would that refresh your recollection?

A Possibly. I don't often browse the broader company privacy policy.

Q Okay. I'd like to show you a screenshot, if I could, of one of Google's web pages that has a list of all of the previous privacy policies in it. Do you recognize that?

A I see that this is the privacy policy's page, yes.

Q Okay. And it's helpful, actually. It includes versions showing track changes, comparing one version to the other. Can you take a look at the bottom of the page and tell us whether Google changed its privacy policy on May 25, 2018?

A That is what the page suggests, yes.

Q And the previous policy that had been in effect since December was in effect since December 18, 2017?

A That is what the page suggests, yes.

Q So if you click on the link for comparison of these two policies, you get something that looks like this. It's a redline of the new privacy policy compared to the old one. Does that look correct to you?

A That is correct, yes.

Q So if we go and we look at this comparison, the previous privacy policy didn't mention Location History by name; is that correct?

A Where's the comparison, sir?

Q Oh, I'm sorry. Can you please turn your attention to what has been marked as Defense Exhibit 43A. This is the same -- you should have a copy of the document. This is the same document we were looking at yesterday. It has the Google web page and link at the bottom.

MR. SIMON: Judge?

THE COURT: Yes.

MR. SIMON: I'm going to object to, I think, the continued insistence despite the witness's consistent answer. He says May 2018 wasn't the first time Location History, to his knowledge, was in a privacy policy. They keep showing him May of 2018, not December of 2017. If defense counsel is insisting upon this, put them both next to him, let him look at both policies, and then he can assess. But I think this redline is -- he's inserting his opinion that the redline, the new words are all inserted as of May of 2018. And there's no indication from just looking at it that that's true. So I'd ask for more context be given to the witness about these two policies.

THE COURT: I'm going to allow him to use this document for whatever it's worth. It doesn't independently show up that the December 18th policy existed without this document in it necessarily. But I think that can be argued one way or the other as far as what inference can be drawn from the document. And you have argued your inference, and they are arguing theirs.

If they have a separate document, then they will respond to your objection, but if this is the one

they're using, then you all will each retain your positions. So I'm going to overrule the objection.

MR. SIMON: Understood, Judge.

MR. PRICE: Thank you, Your Honor.

BY MR. PRICE:

Q So the document that you have here is a comparison of those two provided by Google; correct?

A That is correct.

Q And the crossed out lines, that's the language that was taken out from the December 2017 policy?

A It appears that way, yes.

Q And the language that's not crossed out is the policy in effect as of May 2018?

A That is what it appears to show, yes.

Q I'd like to turn your attention to page 6, if I could. It says --

THE COURT: Let him get there.

MR. PRICE: Excuse me.

BY MR. PRICE:

Q It says at the bottom of the screen there, "You can also turn on Location History if you want to save and manage your location information in your account"; correct?

A That is correct, yes.

Q And that is new language that didn't appear in the

2017 policy; correct?

A That appears correct. One question. Can you go back to the policy's page that you were showing with the comparison?

Q Sure.

A The top of the page. I believe all of this language is captured under "technologies" to the right. I don't know if this is an active page or just a screenshot.

THE COURT: So, I see you're interacting with the screen.

THE WITNESS: Sorry.

A I believe this language is -- it appears very familiar from the technologies section of the privacy and terms. I don't know if this is a screenshot --

Q It's a screenshot. It's not clickable. So long as we're talking about it, it may make sense to ask you, the technologies page that you see here is distinct from the privacy policy part of this page; correct?

A It is a separate section, yes.

Q And the information in the technologies page is not actually in the privacy policy's page; correct?

A I believe that's what was done here with this change, that's correct, yes.

Q Thank you. So, I want to turn your attention back to that redline of the privacy policy and specifically to page 12.

THE COURT: Page 12 now, not page 6?

BY MR. PRICE:

Q So, on page 12, it mentioned Location History one other time. It says, You can turn on Location History if you want traffic predictions for your daily commute or you can save your YouTube watch history to get better video suggestions.

A That is what it says, yes.

Q I want you to take a look at this document and tell me if it says anything else about Location History.

A All 25 pages?

THE COURT: Yes.

Q Yes, please.

MR. PRICE: Your Honor, while we're taking a minute, I wanted to let you know that I'm getting word from my colleagues at NACDL that people on the phone cannot hear what is happening, that they were able to hear at the beginning and that the audio stopped.

THE COURT: Okay. Just a second. We'll call IT. Thanks for letting us know.

(AT&T is called.)

A That appears to be correct. There are two explicit references to Location History in the policy as revised, yes.

Q Thank you very much. And those are both new editions to the privacy policy?

A It appears that (inaudible.)

THE COURT: Wait a minute. My court reporter can't get this while the AT&T operator is talking.

Okay. We'll just take a little break. I'm sorry.

THE CLERK: Are folks able to hear us now?

A VOICE: Yes, we can hear you now.

THE COURT: All right. Has anybody new joined? Do I need to give the same admonition?

THE CLERK: I don't know the answer to that.

THE COURT: All right. I'm sorry. We had a technical drop of the call. I do need to remind anybody, if there are new folks there, that you can't under our Criminal Rule 53 or our standing order rebroadcast, record, or telecast any kind of recording or version of this hearing. Our court reporter is creating our record here.

All right. So why don't you ask the last -- I know, Mr. McGriff, you answered the question. So why don't we start with that, and then we can go

forward.
A There are two -- the two references you mentioned are the two mentions of Location History explicitly in the updated version, yes.
Q Thank you. And those appear to be new editions to the privacy policy?
A That is correct, yes.
Q And the privacy policy doesn't say anything else about Location History other than those two references?
A Yes, the privacy policy appears to include quite a bit of additional information generally, yes.
Q Thank you. So at some point in 2018, what you were calling yesterday the descriptive text for Location History changed; correct?
A What I was mentioning yesterday is that that language changed, I believe, before 2018, yes.
Q The language changed before 2018?
A That is what I believe based on the document you showed me yesterday, yes.
Q You mean the email?
A The email, yes.
Q And did you see the screenshots from yesterday?
A I did, yes.
Q With the old language, the saves a private map

language going through the beginning of 2018 and the saves where you go with your signed-in devices appearing later in 2018?

A I did see those, yes.

Q You would agree that the language changed at some point?

A The language changed at some point within 20- -- at some point from 2017 onward, yes.

Q But you can't say exactly when?

A Not off the top of my head, no.

Q Would it depend on the device that somebody was using?

A It would depend -- after the change is made, there are a host of variables that can impact when a specific user saw that change. As I mentioned yesterday, if I leave here right now and pick up any device that has been sitting on a shelf for three years, the language when that device starts up would be dated to when it was baked into the device.

Q Can I ask you about that? I was confused yesterday when you said that because my understanding is that you would have to be connected to Wi-Fi and signed in to your Google account in order to even be asked about the permissions for Location History. Is that correct?

A You would need to be signed in and connected to opt in to Location History, that's correct.
Q And if you were connected to the internet and signed in, the phone would update itself; correct?
A Presumably, yes, that's correct.
Q In fact, one of the first things a phone does when it connects to the internet for the first time is update itself; correct?
A Not all screens and flows are updated, no.
Q So you can't say which consent flow would have been updated when? It varies?
A Not -- I mean, I don't know how to generalize this statement, but there is not a call to the server for every screen shown in almost any scenario. Some of that will be local.
Q So sometimes it will update with new language and sometimes it won't?
A No. The consent copy will not -- is read from the -- well, again, I shouldn't generalize this. Speaking about Location History specifically, you can find a flow that references Location History, the feature, that is baked into an APK.
Q I'm sorry? What?
A You can find a flow that approaches the feature that says Location History does this. That is

potentially dated. If it is not a screen that we can update on the server remotely, if it's not checking to get updated copy, those stale flows is what I would call it, we block those. So those will not work. There's no way to opt in to that flow, but we are also unable to go and change that screen retroactively because it is already baked into the user interface.

Q So if it's an old consent flow, if it's one that's no longer supported, could Location History be successfully enabled?

A It cannot, no.

Q So, in order to successfully enable Location History, the language would have to be updated?

A A successful opt-in needs to be a flow that is currently supported. If we no longer support the flow, then that opt-in would fail silently, but, again, because it's old. We don't have a way to return a message in the UI to tell the user that it failed.

The user would attempt an opt-in. It would fail silently. The server would say "I have an opt-in request from a dated device." And it will not successfully opt the user in. The user then would notice that this happened only if they then attempted another flow and were once again prompted to opt in to

Location History. The user would realize "I thought I already did," but they hadn't, and that's why they would be prompted again.

Q So we know in this case that Location History was successfully opted into?

A That is correct, yes.

Q So in order to do that, it would have been through the updated consent flow?

A It would have been through a currently supported consent flow, that is correct, yes.

Q And that would have been, at least for the descriptive text, what language?

A I don't know how.

Q Would it be the saves-where-you-go-with-your-devices or would it be the creates-a-private-map language?

A It would be some iteration of the copy that was available at that time. I don't know how I can confirm that. I remember from the research that we did when I filed the declaration that we were not able to determine the specific UI in that case. Something that we've changed since then. We now do track this. But at the time we were not. So we were unable to provide this specific screen of that opt-in at that time.

Q Okay. All right. Thank you.

Even though that language may have changed at some point in time, getting rid of the private map language, Google kept it around; correct? It added it to its 2019 privacy policy January 22. Do you recall that?

A That that specific copy string was used again?

Q Actually, I would like to turn your attention to Defense Exhibit 44. This is another redline showing changes between the privacy policies. This one showing the changes in January 22, 2019. Is that correct?

A That is what this appears to show, yes.

Q Okay. And if we could go down to page 4, please. We see that it says that prior to January 22, with the crossed out language, it says -- it used to read, You can also turn on Location History if you want to save and manage your location information in your account. Is that correct?

A That's correct.

Q The old language?

A Yes.

Q But the new language starting on January 22, 2019, reads, You can also turn on Location History if you want to create a private map of where you go with your

signed-in devices; is that correct?
A That is correct, yes.
Q So the private map language came back in January of 2019?
A I never said that it went away.
Q Well, I meant compared to the descriptive text in the consent flow. It was changed, according to your testimony earlier, that it changed at some point from saves a private map to saves where you go; correct?
A Again, as I mentioned yesterday, we are always looking for ways to further improve and clarify products. That a specific string was introduced does not necessarily mean a previous string was retired. That the decision was made by someone to include one string versus the other here does not suggest that the other string was deemed no longer usable or invalid. The decision here on -- whoever made the decision on which string to include here felt this was the best for this context.
Q In your opinion, is there a big difference between those two phrases?
A Between -- just to be clear, which two phrases?
Q Saves a private map of where you go and saves where you go with your device.
A Big difference? Neither changes -- either would

be appended to the Location History consent, and that text did not change in this period. There seems to be a limited difference in my opinion on these two.

Q Okay. Thank you. So even though it says "create a private map of where you go with your signed-in devices," and this is in the privacy policy, the data that gets saved doesn't get saved just on the device; right?

A No.

Q It gets sent to Google?

A That is correct, yes.

Q Who uses it for advertising?

A We use it at the account level to power quite a few features, yes.

Q And sometimes give it to the government?

A We will always comply with a warrant.

Q Okay. Thank you.

MR. PRICE: Just one housekeeping thing, Your Honor. I would like to move to admit both Defense Exhibit 43A as well as Defense Exhibit 44 into the record.

THE COURT: Any objection?

MR. SIMON: No objection, Judge.

THE COURT: All right. They will be entered.

(Defense Exhibit No. 43A and Defense Exhibit

No. 44 are admitted into evidence.)

BY MR. PRICE:

Q Okay. So I'm sure you're aware that the *New York Times* published an article about Location History in April of 2019.

A Yes, I'm aware of that.

Q So I'd like to show you Defense Exhibit 51. Is this the article?

A This is the article, yes.

MR. PRICE: Your Honor, I'd move to admit Defense Exhibit 51 into evidence.

THE COURT: Any objection?

MR. SIMON: Judge, we would object to entering this article. I think the relevance of it is not there, Judge. And I think it also is basically attempting to enter a legal opinion, various legal opinions, through this article. He can question on it as background information, Judge, but I think, again, this just opens the record to, I think, even the government putting articles in the record that show the efficacy of solving violent crimes using this warrant. I'm just not sure why an article like this is necessary to but in the record.

MR. PRICE: Once again, we're not introducing it for the truth of the matter. We're not going into

any detail about what the article says. Our interest here is in Google's response to it.

THE COURT: All right. Well, I'll allow it in for that limited purpose. It certainly is a public record. I am going to say, Mr. Price, I want you to be consistent about not appearing that you are entering it in for the truth of the matter.

MR. PRICE: I will note that the next time, Your Honor. Thank you.

THE COURT: So the objection is overruled.

(Defense Exhibit No. 51 is admitted into evidence.)

BY MR. PRICE:

Q The title of the article is "Tracking Phones, Google is a Dragnet for the Police"?

A Yes, that is the title of the article.

Q And the article's about geofence warrants like the one in this case?

A That is correct.

Q And it specifically talks about Location History?

A It does mention Location History, yes.

Q Thank you.

MR. PRICE: Your Honor, I hate to do this, but I'm getting word again that the phone line has gone dead.

THE COURT: All right. We're going to need to not continue questioning while that happens. Maybe we can get IT in, please.

(AT&T is called.)

THE CLERK: Can everyone hear us on the call?

A VOICE: Yes.

THE COURT: Can I ask you all, is there something you hear before the phone call drops?

A VOICE: No.

THE COURT: And everybody has dropped off the phone call, not just some?

A VOICE: Yes. I checked with a separate party.

THE COURT: All right. So we're going to call in our IT department and have them checking this hopefully in a way that doesn't interrupt the flow of our questioning here. I have no idea what's happening. We have not had this problem before, certainly with our AT&T system, but because of how we're operating, I need to remind you all that you can't rebroadcast this or record it pursuant to our local rule and our standing order.

Ms. Koenig?

MS. KOENIG: Your Honor, I just stood up because I know that the Federal Public Defender Office

was having a widespread VPN connection problem earlier this morning. And so since we are also connected with the judiciary, I don't know if it's a broader --

THE COURT: I hear the Federal Public Defender was having a widespread blah, blah, blah.

MS. KOENIG: A broader VPN connection problem. So employees are remotely connecting in to our servers. And that was earlier today. I think the systems are separate, but I don't know if it indicates maybe a broader issue with the AT&T connections that are connected with the judiciary as well.

THE COURT: All right.

Certainly, we'll have our IT folks look into it, and we're doing the best -- we do have to keep this process moving. So I'm going to ask you to keep questioning, please.

MR. PRICE: Thank you, Your Honor.

BY MR. PRICE:

Q So, Mr. McGriff, you're aware that the *New York Times* article we were just talking about prompted another email exchange between Google employees?

A Is there a specific change you're referring to?

Q Let me show you Defense Exhibit 37. It's an email chain that begins, I believe, the same day that the *New York Times* article was published.

A Yes, I see that email, yes.
Q Do you recognize it?
A I can't say I recall it specifically, but that is not to suggest that I may not have seen it in the past.
Q You would have been aware of emails responding to the Location History story; correct?
A Sorry. Are you asking me about this specific exchange?
Q Generally. You're aware of the other emails?
A I'm aware that the article was discussed, yes.
Q Okay. And it was discussed here as well?
A That appears to be the focus of this exchange, yes.
Q Thank you.

MR. PRICE: Your Honor, I'd like to move Defense Exhibit 37 into evidence, please.

MR. SIMON: Judge, I'm not going to object because, again, we've let these Google emails in. These are cherry-picked emails from Arizona litigation by Arizona. This particular email has some back and forth expressing legal opinions that not even this witness or any witness that comes before this Court will be able to express.

I think the Court should remove any opinions

about this search warrant that are expressed in any of these emails. And I think this is the email where you will have a lot of back and forth about the propriety of it. And I think, again, it's creating a record in which you have folks who won't testify before this Court, who can't be cross-examined, who are expressing opinions about issues of material fact in this case.

So I would object to this email being wholesale introduced, particularly as it relates to opinions about the geofence warrant before the Court.

MR. PRICE: Your Honor, the relevant opinions in this email chain just relate to confusion over Location History. Again, we're not admitting it for anybody's true statement about what Location History does or doesn't do. Simply to show that Google employees were concerned, confused, and that's all.

THE COURT: So you don't intend to quote this?

MR. PRICE: I do, but not for technical statement or legal opinion.

MR. SIMON: Judge, without that point -- not to continue down this line, but we consistently concede when they make that point, the reality is, Judge, if that is proceeded with in depth, I don't think they can come up with a nontruth-of-the-matter

defense for these emails, particularly one talking about a *New York Times* article addressing the geofence warrant before -- the type of warrant before this Court. They are quoting from the article. Some expressing, Oh, this seems like a problem, and others saying, Well, it doesn't.

I just think this sort of legal discussion in emails in a record of appeal without clarification creates a lot of confusion that I don't think we ought to put into the record.

MR. PRICE: If I quote a statement like that, Mr. Simon can object.

THE COURT: His point is it's in the record, right? His point is that when you put in these documents in full, then it's in the record, and so that anybody reading it would be reading the -- not just, oh, it's for the purpose of confusion. It's that they're saying there's a problem.

I have not read through these emails in depth. I've certainly looked at all of your exhibits. And I am -- I have some concern, especially the way you've been cross-examining this witness by quoting parts of the documents, that it feels as if you are suggesting that the words in the documents are what you are trying to put into the evidence.

What you're having this witness say in response is "I see those words are there." I'm not sure what you're getting out of that.

So I'm going to tell you, I'm going to admit it for the limited purpose, but I'm also leaving open the possibility of it being redacted or removed from the record based on how it is utilized in the future.

But, you know, you're walking a thin line here, Mr. Price. I keep telling you, don't quote the documents as if you are trying to get this witness to adopt what's in them. I know this is Exhibit 224 from the Arizona case. It says that. Everybody is open about it. And the government is recognizing that this is already a public record somewhere. But I can tell you, it doesn't say who's involved. It doesn't say what their position is. It doesn't say in what context that these emails went back and forth. We have no foundation for these emails in this court. And this witness saying "I see that's what this document says" is not moving this case forward very much.

I am hoping that you will convince me in how you are asking questions about these documents in the future that you are not quoting certain quotes here that feel as if you are trying to put in the record

that Google has made admissions. Okay?

MR. PRICE: Yes, Your Honor. The point simply is that --

THE COURT: No, you don't get to summarize the point. You're not testifying here. Either you make the point through the witness or you don't.

All right. Please go forward.

BY MR. PRICE:

Q Mr. McGriff, are you aware that some Google employees expressed confusion over Location History controls following the *New York Times* article?

A I see that's what's discussed in this email, yes.

Q And were you aware at the time that some employees were concerned and confused over Location History following this article?

A I am aware at the time that discussion was had about this article, yes.

Q So when Google expressed confusion on page -- well, this is going to be Bates 63211 to 63212. And that person writes, "I'd want to know which of these options (some? all? none?) enter me into the wrongful-arrest lottery. And I'd want that to be very clear to even the least technical people."

Is that Google employee expressing confusion over the Location History settings and concern?

A I have no idea what, from this snippet, this person was attempting to convey.
Q The person didn't know which of the options were available to disable Location History?
A I don't believe --

MR. SIMON: Judge, I'm only going to say this because I think it's the way that the examination has been happening with this witness throughout. The witness answered that question. He didn't get the answer he liked. He is now going back and asking him the same question again. So is this what he meant? Is this what he meant? He says "I have no idea." I don't know how you get away from "I have no idea." But the objection is asked and answered, Judge.

MR. PRICE: I'll move on.

THE COURT: Okay.

BY MR. PRICE:
Q Could I turn your attention to page 63213? That's Bates 63213.

THE COURT: I'm sorry. What exhibit are you in again? My apologies.

MR. PRICE: This is Defense Exhibit 37, Your Honor. It's page 10 of the PDF, Bates No. 63213.

THE COURT: So it's Exhibit 215 from the Arizona. I misspoke earlier.

BY MR. PRICE:

Q I just want to draw your attention to one other part of this email chain where another Googler responding to the same thread says, "Speak as a user, WTF? More specifically I thought I had location tracking turned off on my phone. However the location toggle in the quick settings was on. So our messaging around this is enough to confuse a privacy focused Google-SWE. That's not good." Do you see that there?

A I see that is what's written here, yes.

Q What's an SWE?

A Software engineer.

Q So this is a Google software engineer expressing confusion over the settings for Location History; is that correct?

A This is a -- what is written here is that this is a Google software engineer. It is not clear to me that they are specifically referring to Location History. The location toggle that's being referenced here, the toggle that appears in settings at the device level is the Location Master which controls location for the device, which is distinct and separate from Location History.

Q Right. He seems to be very confused; right?

A Well --

Q The article that he's responding to is the *New York Times* article which talks about Location History, correct?

A This article talks about location usage and collection, including Location History. This exchange specifically mentions multiple settings that control different levels, what access, and type of location information Google has access to. That statement specifically suggests, from what's written here, does not suggest that it's explicit to Location History.

So I would say, yes, this is a Google software engineer expressing some thoughts on a location toggle, which is not specified to be Location History in this context.

Q Okay. Thank you very much.

You're aware that the *New York Times* article prompted another congressional inquiry; is that correct? In 2019?

THE COURT: Can we be specific? You have now introduced a second *New York Times* article; am I right?

MR. PRICE: No, this is the only *New York Times* article.

THE COURT: It's all April 15?

MR. PRICE: Yes, Your Honor.

THE COURT: Just a different version. All right.

THE WITNESS: Which inquiry are you referring to?

Q Can I show you Defense Exhibit 54, please. Shortly after the *New York Times* article ran, the House Committee on Energy and Commerce sent a letter to Google's CEO on April 23, 2019. Is that correct?

A That is what this exhibit shows, yes.

Q And this is the letter that was sent to Google's CEO?

A That is correct, yes. Can I ask one clarification?

Q Yes.

A When you say "inquiry," you mention that you also -- there was another inquiry you mentioned yesterday. What do you mean by "inquiry"? Just a general outreach with questions or do you mean something more formal?

Q I don't think I had a specific definition. This letter expressed some concern about Sensorvault and the database Google uses. That's the database Google uses to store Location History?

A That's correct, yes.

Q Thank you.

Following the *New York Times* article, Google made even more changes, some of which you discussed in your blog post; correct?

MR. PRICE: Excuse me, Your Honor. I would move to admit the House letter into evidence for the limited purpose of its existence.

MR. SIMON: Judge, we're going to object on relevance grounds, not merely hearsay. I think beyond that, Judge, in the interest of fairness, defense counsel, at the very least, ought to find Google's response to these questions and put it in the record as well if we're going to put this letter in. And we at least have that with the Senate letter that also wasn't relevant, but they are questions directed to Google that they -- if we're going to put sort of hearsay into the record on this point, that would be helpful. But the objection is relevance. I don't see the point of congressional leaders asking questions to major corporations, how that plays into this hearing.

THE COURT: So, I'm going to overrule the objection as to purported relevance. It's clear that the defense has a theory that either it's going to shore up or not with respect to how Location History notifications or operations changed.

I do agree, though, that -- so it will be for

establishing its relevance in greater context later. And for the limited purposes that we're talking about. I do agree, though, that in fairness, the answer should go in absent objection from Google.

And so you sent in a Senate inquiry also, and I think some of the responses were there. But I want you to work with the Assistant United States Attorney and counsel for Google about whether or not they want to shore up any responses. That strikes me as a more fulsome record than what you've offered, and you don't necessarily have to offer that, but now that it's been raised, I think we should close the loop. All right?

MR. PRICE: Thank you, Your Honor.

Just to clarify, the Senate letter was a request to the FTC for an investigation.

THE COURT: Right. Right. Well, the responses that you submitted were responses to what?

MR. PRICE: The request for an investigation included an attachment, which was a previous letter that Google -- that the senator had sent to Google seeking further clarification.

THE COURT: All right. So, I'm going to have you all agree. That's the problem with this, Mr. Price. Right? If they are using the phrase "cherrypick," you are allowed to advocate, but if you

get called on it, I'm telling you, make a full and fair record. So I'm going to allow you all to caucus about that, and then place on the record what your decision was or Google's position is and then I will make a final ruling.

MR. PRICE: Thank you.

THE COURT: Thanks.

BY MR. PRICE:

Q Okay. So we've got the *New York Times* article as well as the AP article we talked about the day before, the year before --

THE COURT: I was thinking the AP article. I've got it. Okay.

BY MR. PRICE:

Q And in response to this feedback, was this the feedback you were describing in your blog post when you talked about some of the changes that Google was making to improve Location History?

A These are a few of several signals of feedback that we receive on a regular basis, yes.

Q Okay. Thank you. As a result of that feedback, Google made some more changes to the way Location History functions, the controls for users?

A I am not aware of a point in time in the life of the product that we have stopped making improvements

and changes to the product.
Q Okay. One of those changes that you made was the new auto delete function that you wrote about in your blog post; correct?
A Auto delete was not a change specific to Location History. It was rolled out at this point to several Google products, yes.
Q But it applies to Location History?
A It does apply to Location History, yes.
Q And in your blog post, you were discussing it in the context of Location History?
A In the blog post, it's discussed both in the context of Location History and search.
Q Okay. I want to ask you about that deletion process, though.
A Yes.
Q Even if a user deletes their Location History data, it doesn't get deleted immediately, does it?
A It's near immediate.
Q There's a deletion process?
A That is correct.
Q And Google doesn't confirm that using Google's tools for deleting location data will actually delete that location data, does it?
A Can you clarify what you mean by confirm?

Q Sure. Let me show you Defense Exhibit 45. It's the October 29, 2019, privacy policy redline, track changes version.

THE COURT: I'm sorry. What exhibit again?

MR. PRICE: Defense Exhibit 45.

BY MR. PRICE:

Q It says Google added a caveat to the -- I want to turn your attention to the "retaining your information" section of the privacy policy.

MR. PRICE: And for the Court, this is on page 15 of the PDF. The pages are not internally numbered.

BY MR. PRICE:

Q There's a section there that says "Retaining your information"?

A Yes.

Q And this is a new section that was added based off of the track changes that you see?

A Expanded?

Q Added. Added.

A The crossed-out copy here --

Q That's the old language. And the non-crossed out copy is the new language.

THE COURT: You know what? He is saying it's expanded. And I think you can understand that what he

means is that this is longer text than was there previously. And so bantering with the language with your witness --

MR. PRICE: Maybe I misheard him. My apologies. Excuse me.

THE COURT: What?

MR. PRICE: This is -- just that this was, this language wasn't there before. That's all.

THE COURT: But that's not how you're examining him. So the way you cross-examine somebody, without injecting your own opinion necessarily, is you say that there's a paragraph that is blocked out; correct? Correct. Is it anywhere else in the retaining your information? No. Are there paragraphs that are not blocked out? Yes. Would that possibly be new information?

You don't banter with him about the answers that he's giving you. The answers that he has given you are the answers that he has given you. You cannot inject functionally your own opinion about which word is right. You can cross-examine him so he adopts it, but you cannot inject your own opinion. Okay?

MR. PRICE: Yes, Your Honor.

BY MR. PRICE:

Q I would just like to turn your attention to the

language that says "When you delete your data, you follow a deletion process." Do you see that there?

A Yes.

Q It says, "We follow a deletion process to make sure that your data is safely and completely removed from our servers or retained only in anonymized form"; is that correct?

A Yes.

Q And when it says "retained," that's a little bit different than "deleted," isn't it?

A That somehow the transformed data is retained. There's a subtle difference there. It notes that it's only an anonymized form.

Q So it gets deleted through the deletion process but retained in anonymized form?

A The privacy policy is the privacy policy for Google. For Location History, it is deleted. This is generalized to speak to the company-wide policies and practices. In the case of Location History specifically, it is deleted.

Q So it's deleted from the Location History database?

A That's correct, yes.

Q But it's retained in a different database?

A No, that's not correct.

Q In anonymized form?
A No. So, this policy speaks to Google's broader company-wide policies. What this is specifically noting is that in the deletion process, some information might be retained in anonymized form. What that's referring to is not explicitly referring to Location History.

Location History information is also deleted by a process. There's a single store for that, as mentioned in the last exhibit, Sensorvault. That deletion is permanent and final.

Q Where is anonymized data that's retained, stored?
A I can't speak to the broader company policy and what specifically they're referring to there. It's a data type that is outside of my scope.
Q Okay.

MR. PRICE: Your Honor, I would like to admit Defense Exhibit 45, the privacy policy, into the record, into evidence.

MR. SIMON: No objection, Judge.

THE COURT: All right. It will be entered.

(Defense Exhibit No. 45 is admitted into evidence.)

THE COURT: I'm going to say a couple things. I'm hearing something.

THE WITNESS: I am, too. It's like a radio.

THE COURT: Yes. And I want that to stop. What am I hearing?

MS. KOENIG: Your Honor, I heard a little bit of something like that yesterday, too, and I'm wondering if perhaps maybe somebody who is on the audio feed may not be fully muted. I'm not sure.

THE CLERK: I can mute our mics.

THE COURT: No.

THE CLERK: Their mic. Not us. Anything coming from that.

THE COURT: I'm going to say, if there are folks on the AT&T line who are talking, we can hear you, and it is disruptive. If you're in my courtroom here in person, you're not rude enough to speak over any witness who is testifying. We don't allow it in this court. And I'm going to tell you all, either you pay attention and you listen or you don't. I'm still hearing it. What is it?

MS. CARROLL: I'm being told the audio has gone out again on the phone line. So I don't know if maybe they can't hear.

THE COURT: Maybe they're talking about the fact that it's gone out.

All right. We're going to take a recess and

figure this out. I am going to say also, I want counsel table to be a little less vocal. I don't want people commenting on the type of examination that's happening where I can hear it.

I don't want -- Mr. Chatrie, you're allowed to speak to your attorney as much as you wish, but you have to understand there are a lot of microphones there, and it becomes background noise.

So, Mr. Gill, I'm just going to ask you -- I don't want you not to talk to your client, of course, but you have to step away from the microphones a little bit because it is disruptive to what is happening in our courtroom, and it's not fair to Mr. McGriff or to Mr. Price that he is distracted or that I am, and not looking at the right exhibit because I get concerned about the demeanor and the professionalism with which we're handling this case.

So I want somebody to tell the AT&T folks, if you know, them tell them to hush. And I will remind them, but we're going to take a 15-minute recess, and my hope is that we will just get the testimony in efficiently and fairly and without disruption.

All right.

(Recess taken from 10:10 a.m. until 10:35 a.m.)

THE COURT: All right. Well, welcome back.

Let me just put on record I'm pretty glad we're not doing this by ZOOM, since we have everybody here and are still experiencing technical difficulties.

Can I ask if anybody on the AT&T line can hear me? So that is a no. So let me say this: We cannot let this AT&T line trip us up like this. We are open. I want to accommodate this, but our courtroom is open, and we have a satellite courtroom that we may not be running today because no one showed up yesterday. But if people were to show up, you can come on in. You're welcome to do it. But this is far too many distractions. And it's not anybody's fault.

And so I'm going to ask those of you who are in touch with folks, let them know we're just going forward. They're welcome to come on down here and listen and do what they want to do. But this is, you know, we're an hour and 40 minutes into this proceeding, and we've gotten maybe 40 minutes of testimony, maybe 30. It's not appropriate for Mr. Chatrie, for our witnesses, for counsel here.

And so I am a fan of the First Amendment, but we cannot let this proceeding be driven by folks who want the courtesy of an AT&T line when we are fully open and operational and they can come in here.

I don't know whether or not it's those folks talking. I am going to just ask them not to if they get back on. We have our IT working on it. They're working with AT&T. We have checked. Sometimes our CSOs have walkie-talkies. It sounded a little bit like that to me, but none of them are using them. So I don't exactly know what's happening. It's quite possible there are lines crossing, I would think, because we keep getting jumped off of AT&T.

But I want to confirm, especially those of you who have colleagues, that you don't object to our just going through this when your colleagues can't hear it.

MS. KOENIG: Your Honor, from the defense's perspective, we are absolutely in agreement that we need to move forward now.

THE COURT: All right.

MR. SIMON: Likewise, Judge. We're ready to go.

MS. CARROLL: Likewise for Google, as well. Thank you.

THE COURT: All right. Okay. We'll work on it, but let's be productive. We'll continue the examination.

Obviously, Mr. McGriff, you're still under

oath. I have to say it every time.

BY MR. PRICE:

Q Mr. McGriff, I'd like to call your attention back to Defense Exhibit 47. This is the second blog post that you wrote. In addition to adding the auto delete feature, you also wrote in your blog that "It's our goal to help you stay informed about your Location History"; correct?

A Yes.

Q And you said, "If you have chosen to turn Location History on, you will receive periodic email reminders that let you know what data you are saving and ways to manage it"; is that correct?

A Yes.

Q And then in your third declaration, which is Defense Exhibit 23, you also wrote about this. You said that Google sent monthly timeline updates to some users; is that correct?

A That's correct, yes.

Q And one purpose of those updates was to remind the user that the Location History setting is on?

A Among other things, yes.

Q But Google, again, in your affidavit, pages 8 to 9, you wrote that Google has no records reflecting that such emails were sent to Mr. Chatrie.

A We do not retain records for that long for emails sent, that's correct.

Q So you said that one reason for that "could be because no such emails were sent"?

A That is possible, yes.

Q But you don't know why?

A Again, for the life of the product, we have steadily made improvements. We have steadily expanded the suite of emails that we send related to the product. Because of the way we record the emails that are sent in this context, this is too far back for us to say with certainty which emails were or were not sent for a specific account.

Q Thank you. I'd like to turn your attention now to Defense Exhibit 7, the third page. This is a screenshot of the opt-in screen when first setting up Google Assistant. I want to just go through with you here some of the terminology because I feel like we're getting tripped up a little bit.

The line -- you've used a few different terms to describe what we're seeing here in terms of text on the screen. But the line right underneath where it says "Location History," in this case it says "creates a private map of where you go with your signed-in devices," that's the descriptive text?

A That's the way I would describe it, yes.
Q Okay. And if you hit that little triangle next to Location History, that's the expansion arrow?
A That's correct, yes.
Q And can we go to page 4. If you hit that expansion arrow, then you see what's on that screenshot on the far right-hand side, what you've been calling the copy text; is that correct?
A That full block there, that is the Location History consent, yes.
Q So you call that the Location History consent?
A That is the consent copy, yes.
THE COURT: Wait. Are you on page 3 or 4? Is this where we --
MR. PRICE: This is Figure 3, and I believe it's on page 4.
THE COURT: It's on page 3.
MR. PRICE: Page 3, I'm sorry. Yes, page 3.
BY MR. PRICE:
Q So that block of text, that's the consent copy text?
A It's the Location History consent, yes.
Q The Location History consent. Okay. So then can we go down to the next screenshot, please, on page 4. Further down.

So, what -- do you see those buttons? One says "No, thanks" and one says "Turn on"?

A Yes.

Q What are those called?

A That is how a user would accept what's above. So their dynamic. As you did in the previous figure, you showed when a user first lands on that screen, you can't turn it on from that screen alone. Your options as the figure shows are "Skip" or "Next". If the user says "Skip," they are skipped. They won't see the subsequent screens. If the user says "Next," then they're shown what you highlighted in Figure 3. And then if the user scrolls down, they will see the "No, thanks" or "Turn on." So those buttons are dynamic.

Q And the only way that you see the consent copy text is if you click on that expansion arrow; right?

A That's correct, the expanded copy, that's right.

Q So you don't actually have to see it in order to hit "Turn on"?

A You have to scroll to the bottom to click "Turn on," yes.

Q But you don't have to see the consent copy text?

A You don't have to expand it there, no.

Q And this whole process, is that referred to as the consent flow?

A That is a consent flow, yes.
Q So this process is a consent flow?
A That is a consent flow, yes.
Q Thank you for clarifying that.
The text -- if we could go to the screen that shows the consent copy text, please. Thank you.
So this text that you see here, that's consistent, in fact, the same as the text that you provided in your third declaration; correct?
A Yes. Yes, it is.
Q Okay. But it looks a little bit different in screenshot form than it does in plain text. Would you agree with that?
A What do you mean?
Q Well, laid out like this in this format, you know, with the copy text hidden behind the expansion arrow, it looks different than just writing out the text on a piece of paper; correct?
A This is, again, a fully dynamic flow. So, yes, it looks very different when you freeze on individual screens and break it out in this way, yes.
Q So, could we go down to the "Turn on" button. So the "Turn on" button there is highlighted in blue by default?
A So, it starts off not visible, but once the user

interacts with the page and scrolls to the bottom, yes, that button appears in blue.

Q And the "No, thanks" button is not highlighted in blue. It kind of blends in there?

A The "No, thanks" button is not captured in a blue box, no.

Q Thank you. And this consent flow for Google Assistant, this looks different than the consent flows that you provided in your third declaration for Google Maps; correct?

A Again, in any of my declarations, I never attempted or suggested that I was presenting an exhaustive exploration of all of our opt-ins.

Q Understood. It looks different from the consent flow that you showed for Google photos as well; correct?

A This is a variation on a theme of that flow, that's correct, yes.

Q And this variation, instead of asking the user to just enable Location History, there are two other permissions on the screen; is that correct?

A Again, this flow is dynamic. So if a user saw the -- in your Figure 3, in this exhibit, if a user saw the prompt to set up Assistant, if the user skipped, they would see none of the subsequent

screens. If the user said "Next," they would then see whichever permissions they had not already consented to for the account that were required for this particular feature. That is unique to this particular flow, that is correct.

Q So if you're setting up Google Assistant for the first time, and you have never enabled Location History, you've never enabled device information, and you've never enabled Voice & Audio Activity, you would see all three permissions on this one screen?

A At that time, that was the case, yes.

Q If you would say "already enabled device information" for some other reason, it wouldn't show up here?

A That is correct, yes.

Q If I had enabled device information and Voice & Audio Activity, it would only show, say, Location History?

A Correct. If you had not previously opted in to Location History, yes, that's correct.

Q When you group permissions like this together on one page, it's called bundling; right?

A I don't know what its official term would be. I casually, yes, do often refer to these as a bundled presentation, yes.

Q And bundling can make users share information that they otherwise wouldn't; correct?
A I don't know that that's true.
Q Well, if a user doesn't agree to everything here, then Google would block off access to Google Assistant?
A I don't believe this would prohibit or prevent a user from using Google Assistant.
Q So you're saying it's possible to enable Google Assistant without -- enable Google Assistant for the first time without enabling all three of these permissions?
A I am not the assistant PM, but I don't believe you would be -- I couldn't say that that service would completely block you if you did not consent to all of these.
Q If you click "Turn on," then it enables all three; correct?
A If a user went through the flow and scrolled to the bottom, yes, they would be able to turn on and enable all three, that is correct.
Q And the only other option is "No, thanks"?
A "No, thanks," that's correct.
Q And if the user clicks "No, thanks," is Assistant set up?

A From this particular flow and these screenshots, the user could skip it entirely. The user could scroll through and say "Turn on" or the user could scroll through and say "No, thanks". I am not the assistant PM, and I do not recall what restrictions they had on usage. I would be surprised if you weren't able to use it at all, but, again, I'm not the assistant PM.

Q But you would agree if you clicked "No, thanks," Assistant will not be set up at that time; correct?

A It may not be completely set up, but, again, I would be surprised that would you be blocked from using the feature.

Q Does it say that on this page anywhere?

A Say what specifically?

Q That it might be possible to use the feature without clicking "Turn on"?

A It does not say -- again, this is a dynamic screen. So it would appear different for the user based on whatever their account configuration was. It is possible that a user approaching this screen, for example, had already consented to device information and Video & Audio Activity, in which case they only saw Location History. I am not the assistant PM. I don't recall that Assistant would have blocked you if

you said no.
Q Well, you could set it up later, of course; right?
A You could set it up at a different point.
Q But you'd see the same screens, the same consent flow?
A That I couldn't say. I am not an expert on Assistant.
Q You would agree that Location History here is an account level setting? That means if you enable it here, it is enabled for all devices across your entire account?
A No. If you opt in to Location History here, Location History and Location Reporting would be enabled on that specific device. But if you were signed into multiple other devices, Location Reporting would not be enabled on those devices. So their Location History was on for the account. Those devices would not actively be contributing to your Location History.
Q But if you had one device, and you turned it on in this way, it would be on for everything on the phone; correct? On that device?
A Yes, if a user opted in to Location History through this context at this point in time, July 2018, Location History would have been enabled on their

account. And with that, seven days later on that same device, they would see the warm welcome, as we call it. Everything would have been enabled on that device, yes.

Q So it doesn't have to be an account level setting, does it? In other words, it's possible to have Location Reporting only for apps that are actively using a user's location? This is the way that an iPhone does it, for example.

A I'm not sure that I follow that.

Q IPhone users can choose to give an app permission to use location services only when the app is in use. Are you familiar with that?

A I believe you're conflating Location History with location services. The same is true on an Android device. A user can choose which app has access to location on the device. Those are the app level run time permissions, yes.

Q So on an iPhone, you can restrict it to one app or another?

A On both Android and iPhone, and I believe every other phone manufacturer, you can restrict location access at the app level, that is correct.

Q And Location History specifically?

A Location History is not location services for the

device.

Q Correct, but I'm asking you about Location History.

A But you're making a false equivalency with what's happening on an iPhone. On both iPhone and Android, there are runtime permissions that control whether or not an app has access to location in the background.

On both iPhone and Android, a user can decide whether or not an app, a specific app, has access to the location in the background or only in the foreground. Those are app level permissions. They are not tied to Location History.

If a user enables Location History for the account, in the context of Android specifically, that information is collected and stored and used in Location History at the account level.

Individual apps can access Location History information, but by policy we do not allow those apps to use Location History as a workaround, for example, for current location.

So, if a Maps user says "no, Maps, you cannot have my location permission," Maps cannot call Location History and say, Tell me where this user is. Yes.

Q Okay. Thank you for clarifying.

We talked about this a second ago a little bit,

but if a user goes through and sets up Google Assistant in this way, and then later goes and pauses Location History, Google Assistant will still continue to function; correct?

A Yes, that is correct.

Q But Google doesn't inform the user at the consent flow stage that that is a possibility; correct?

A Again, the consent flow is dynamic. So a user may or may not be presented, depending on their own account activity prior, with any of these options in the menu. So what is presented to the user in the context of seeing this specific flow would, again, be based on the user's previous activity across Google products and services.

Is the ask to generalize, then, across all users?

Q No, no. I'm actually asking if you can point me to where in the consent copy text it says that the feature, in this case Google Assistant, would still function even if you pause Location History.

A I don't see in the copy text that it either says the feature will or will not work if the user does not proceed with any of the steps, the various options of this flow.

Q To pause Location History, you can only do that once you've enabled it through the settings panel;

right?

A What are you referring to as a settings panel?

Q The settings app on an Android phone.

A Are you referring to a specific point in time or just generally?

Q After it has been enabled.

A So, after Location History has been enabled at the account level, the user can go through the settings on any particular app that uses Location History, so it has Location History powered features. The user could go through the device level settings on an Android device, and the user could also go to myactivity.google.com where they can view all the activity controls and suspend it there.

So you can either do it directly on the device at the settings level through an app on a device, any device that you're signed into, or on a desktop, any laptop, myactivity.google.com and make a change there.

THE COURT: So, Mr. McGriff, myactivity.google.com is really familiar to you, but my bet is it's really hard to transcribe as quickly as you say it, especially with all the dots and stuff. And using phrases like "I'm not the PM," just presume that not all of us knows what a PM is. So I'm going to ask you to clarify that. I think I know what it

is, but especially with things you're super familiar with, those things come out fast from any human being. And I'm just speaking on Ms. Daffron's behalf.

THE WITNESS: Got it. For reference, "PM" is product manager. So I'm not one of the assistant product managers. And the site specifically I've been referring to as myactivity.google.com is the main settings page where you can view all of your account level settings and manage them, and that can be done either through a mobile browser or on a desktop.

BY MR. PRICE:

Q So a user would have to actively, intentionally navigate to that, settings, either through the app, through the settings panel, or through that website that you just gave us?

A That's correct.

MR. SIMON: Judge, I think the answer's fine because he said yes, but I was going to ask to break that down because there are a number of different topic areas there in that question.

THE COURT: You mean, it's a compound question?

MR. SIMON: Correct, Judge. My apologies. That would be the objection, compound question.

THE COURT: It also seems to repeat what the

witness was saying. But are there more than three ways to change the Location History setting other than the three you just talked about?

THE WITNESS: Those are three paths, the three paths that would be possible, yes.

MR. PRICE: Thank you.

BY MR. PRICE:

Q So, if a user takes one of those paths and they find the setting to pause Location History, Google provides a pop-up screen at that point; right?

A There is a screen that explains -- there's a screen that explains what is happening with that pause of the service, yes.

Q Thank you. Could I draw your attention, please, to Defense Exhibit 27, specifically pages 22 to 23.

THE COURT: I'm sorry. Remind me of the exhibit number again, please.

MR. PRICE: Exhibit 27, Your Honor.

THE COURT: How about you put on the record what we're looking at aside from the number, please.

Q Mr. McGriff, can you tell us what --

THE COURT: No, you can just put it on. It's already in evidence.

MR. PRICE: Sorry. This is Defense Exhibit 27 at page, I believe, 23. And this is the screen

that pops up if you attempt to --

THE COURT: I mean name the article, sir. I'm sorry. I'm not being clear.

MR. PRICE: Oh, I'm sorry. This is the report from the Norwegian. It's called "Every Step You Take."

THE COURT: All right. There we go.

BY MR. PRICE:

Q Is this the screen that would come up if you successfully found a place to turn Location History -- to pause Location History?

A In any of the numerous paths that a user could take to pause the setting, yes. This would be the pause copy that appeared at that time, that's correct.

Q Great. So attempting to pause the service results in this warning that says it "limits functionality of some of Google's products over time, such as Maps and Google Now"; is that correct?

A That is correct.

Q But there isn't a comprehensive explanation of all the services that would be affected; correct?

A That is correct, yes.

Q It just mentions those two. It doesn't mention Assistant?

A This was not meant to be exhaustive, that's

correct, yes.

Q And it doesn't explain actually how the functionality would be limited for any of those specific apps?

A As mentioned previously, Location History is used and in quite a few products and services and what would be impacted would be wholly dependent on what a specific user was utilizing in their sort of experience across Google products and services. The copy here is not meant to be exhaustive or describe what every user would experience in terms of change in service, because that would be near impossible. The screen would have to be -- well, not impossible. The screen would have to be dynamic and specifically say what was happening in that case.

In this case, it's clearly illustrated. It just has, you know, these would be impacted, such as these would be impact services.

Q But it does not say how the functionality would be limited?

A It does not explicitly say that, no.

Q Okay. Thank you.

I'd like to take a closer look at some of the screenshots for this consent flow process for Assistant. If we could turn to Defense Exhibit 7 at

page 4 again, please.

MR. PRICE: Can we show the one with the copy.

BY MR. PRICE:

Q So this is page 3 of Defense Exhibit 7. And, once again, we have the descriptive text in the Location History that says "Saves where you go with your devices"; correct?

A That's correct, yes.

Q And then the consent copy text on the right-hand side.

A That's correct, yes.

Q That can only be viewed by clicking that expansion arrow?

A That is correct, yes.

Q So it requires extra clicks, at least one, here to learn, for example, that your Location History data is saved with Google and not on your phone?

A Location History is only available through Google. Who else would it be saved with?

Q Well, the descriptive text says "Saves where you go with your devices"; correct?

A Sorry. Is the suggestion that the descriptive text is suggesting that it's an on-device feature?

Q I'm saying it does not specify one way or the

other, does it?
A I apologize. I don't believe any of our settings, any of the controls mentioned here explicitly say -- make a distinction of server versus on device.
Q I understand that that is how it works now, but as a user, where would the user find that information on this page?
A Just to be sure that I'm clear, you're asking where would a user know that this information is being saved with Google on Google servers versus on the device locally?
Q Correct.
A That is not a distinction that is made on this page, no.
Q It's made on the next page, on the consent copy page?
A That is not a distinction of note in the consent copy. It is there, but it is not in any way meant to like -- the distinction of whether data is stored on a device locally or on the server is -- I apologize. I don't know how to respond to that. It is more -- it is noted in the consent copy, yes.
Q Okay. But not in the descriptive text?
A No.
Q Similarly, it would require an extra click here on

that expansion arrow to learn that data is being saved even when you aren't using a specific Google service; correct?

A On this page, yes.

Q And it requires an extra click, same one, for a user to learn that location data is sent to Google even if the internet connection becomes disabled?

A Sorry. What are you referring to? Oh, I see. Sorry. Yes, that is correct.

Q Thank you very much.

So that consent copy text also says some things like Location History helps give -- helps Google give you more personalized experiences; right?

A Yes.

Q Like a map of where you've been?

A Yes.

Q Tips about your commute?

A Yes.

Q Recommendations based on places you visited?

A Yes.

Q And useful ads?

A Yes.

Q Those are all positive things from Google's point of view; correct?

A Yes.

Q They're intended to explain why users might want to enable Location History?
A That's correct, yes.
Q But there isn't any mention here about how frequently Google collects Location History information, is it?
A There is no statement here about the frequency of collection, that is correct, yes.
Q And there's no mention of the quantity of location records that Location History generates; correct?
A There is no statement here, no, that's correct.
Q And there's no mention in that consent copy text that Assistant will work without Location History enabled?
A There is no mention that any of the products or features mentioned here will work without the setting enabled, that is correct.
Q Thank you. So let me shift gears a little bit. Let's say I'm a user who does not want to have Location History enabled on my device. To keep Location History off, I have to go through a bunch of different steps, starting from the beginning, the initial setup of the phone; correct?
A Again, the majority of users do not have Location History enabled. For those users who have Location

History enabled, yes, to turn it off, they can take any of the numerous paths I mentioned before, yes.

Q No, I guess what I'm saying is it starts off as off. The default when you start up a new phone is off; correct?

A Location History -- well, Location History is an account level setting. Yes, it's an account level setting, and it is off by default.

Q The default is off when you start up a phone, but at least in 2019, the very first thing that would happen after you went through the initial setup and agreed to the terms would be a prompt to enable Location History; correct? Sorry. A prompt to enable Google Assistant; correct?

A In 2019?

Q I'm sorry. July of 2018.

A In 2018, at the beginning of the year, yes, if you set up Google Assistant, you would be presented with the Location History consent if you had not already opted into the service, yes.

Q After you do the initial setup of the phone, that screen, "Meet your Google Assistant," comes up immediately or came up immediately in 2018?

A I cannot speak to exactly when that appears in device setup or under what circumstances. But

assuming a user got to this screen, yes, this would have been the flow, that's correct.

Q And, obviously, this prompts the user to enable Location History?

A This particular flow, yes, it does.

Q So, in order to keep Location History off, the user would have to skip the step and decline enabling Location History?

A Which, again, the majority of Google accounts do not have Location History enabled.

Q Okay. After that initial setup process, during the first use of some applications, there's also a prompt to enable Location History; correct?

A For some products that have Location History powered features, yes, that's correct.

Q So, for example, Google Maps, the first time I open up Google Maps with my new setup phone, it's going to ask me to enable Location History; correct?

A Under some set of circumstances in the context of Google Maps at that time a user would have been prompted. The notification was -- there's a notification priority and depending on the user's activity and behavior, the user may or may not have seen that notification, but, yes, it was a possibility.

Q So, then, to keep Location History off, I would have to decline activating it through Maps, as well; right?

A That is correct.

Q And the same thing with Google Photos; correct? The first time you open Google Photos, there's a prompt to enable Location History for Google Photos Places; is that correct?

A I'm not aware that that was featured in the same way that it was featured in Maps, but for both, again, I would say yes, presented as an option, which the majority of our users do not opt into.

Q So, again, if I wanted to keep Location History off, I would have to decline the invitation to turn it on when using Photos for the first time?

A Yes. The majority of our users would have declined that, yes.

Q And long pressing the home button on an Android phone, that would also bring up the Google Assistant app; correct?

A In 2018, I believe so, yes.

Q And so if a user hadn't enabled Assistant during that initial setup process, they would be prompted to do it when they pressed the home button with the long press?

A I don't know under what circumstances a user would see this specific Assistant flow. Specifically, as mentioned before, I'm not sure -- I can't say that this specific flow would be the one shown at a subsequent point.

Q But there would be -- if Assistant is not set up, the first time it comes up, you would see these screens; correct?

A I couldn't say definitively, actually.

Q Okay. In any event, to keep Location History off from the beginning, a user would have to say no multiple times; correct?

A No, it would depend entirely on what a user's activity actions, and across Google products and services.

Q So the user would have to decline the invitation to set up Google Assistant initially; correct?

A Assuming that a Google user saw that, yes.

Q The user would have to decline the invitation when opening Maps for the first time?

A If the user was prompted with that opt-in flow, then yes.

Q And the user would have to decline it when using Google Photos for the first time?

A Again, across all products, that user Location

History, if a user was prompted contextually to opt-in with a Location History powered feature, then yes, the user would be presented with the option to say yes or no.

Q Then, again, if Google Assistant came up for some reason, perhaps a long press of the home button, they would have to decline the invitation to set it up then, too; right?

A That's the one I'm not sure about. I can't say whether or not Assistant had the same flow for that same type of behavior at that point.

Q So, at least three times, maybe four?

A No. Again, I disagree. A user may not -- what a user is presented with would depend entirely on the user's behavior. Not every user uses Google Maps. Not every user uses Google Photos. So it is very possible that a user saw -- for example, this flow would have required the user to have a connection. The user may have set up their device with no connection, in which case they wouldn't have been presented with the Assistant flow.

Device and their connection could mean no send, no Wi-Fi, but in that scenario, the user would have seen none of these prompts.

A user could have gone through this initial flow

and then never opened Google Maps and then never opened Photos. They wouldn't have seen the other ones.

So I can't say that a user -- the number of times definitively that any user would have seen any of these prompts, but I can say yes, these would have been the prompts that were available at that time.

Q So, a user who did use Google Maps and Google Photos would have been prompted in this way at least three times; correct?

A Could have been prompted. Again, all of these are dependent on the user's activities. There are more important things happening in Maps, for example. So if you are in an active navigation session shortly after first opening Maps, no, Maps would not prompt you with any opt-in request because you are in the active task completion mode. The prioritization of that screen would have been too low to warn it to be triggered at that time. So it is a potential option, but it's impossible to say to what percentage of users and what flow and so forth.

Q So it's at least possible that a user would have to decline the invitation to enable Location History multiple times in order to keep it off?

A Yes, it is possible that a user would have seen

the option to opt-in multiple times, yes.

THE COURT: I'm pretty sure we've covered that territory multiple times. Let's move on.

BY MR. PRICE:

Q Does this increase the chances that a user might turn on Location History by accident?

A It is always possible that a user goes through a flow, might not fully understand or wants to revisit. For that exact reason, in 2017, we introduced what we call the warm welcome notification for any user who opted in to Location History from Q4 2017 on, we triggered a notification in Maps. It triggered seven days later.

Seven days was chosen because we thought at that point we would have sufficient context of a user's activity from a week since turning on the control. And the notification said -- again, it was the warm welcome. Hey, Location History is on for your account. Any interaction with that notification brought the user into Timeline where the user would be able to view all the information that we had collected, including the activity, the trips, the places.

The hope in introducing that was that even if a user didn't have full context or full understanding

about the points you've previously made, the granularity of the information, or the type of information, that the collection was happening passively, like, for example, while driving, that we understood the nuance of activity recognition.

The visualization in the Timeline UI, user interface, was very explicit and clear. So that warm welcome notification was so that a user would see it seven days later, click through, see in full context, and might say, This is not what I intended. Turn the control off. There you can access again through the app Timeline. You can turn Location History -- you know, pause Location History there.

The user could also -- we present a full suite of controls. This is well before auto delete. But at the time we had delete by day, delete by data range. All of those controls were made available in the context of Timeline.

Again, because every product is steadily evolving, I realize some users would not see the notification. So we now send a warm welcome email. So, again, this speaks to that suite of emails that we send. So seven days after turning Location History on, we now send an email in addition to the warm welcome email notice because not every user will see the maps notification.

Again, not every user uses Google Maps.

So the thought was if you had turned on Location History in a different context, you may not see the Map specific notification. So now we send the email with that exact same content.

That email features prominently at the top direct links to turn Location History on or off. And in that email, we specifically provide a snippet or insight into the data that's been collected for the first seven days that the user has had the control on.

Again, this is all to address the point you're making, that a user might turn it on, and then either not realize the scope or exactly what's collected, and we wanted to provide that additional context.

Q Thank you. I just wanted -- that was a long answer. It is the case, based on what you just said, with some qualifications that --

MR. SIMON: Judge, I'm going to object to a continuation of asking the witness to speculate about possible accidents. But I also think this is, again, going to be a question preemptively that's been asked and answered.

MR. PRICE: I would just like to get a yes or no to my question, because I appreciate Mr. McGriff's answer, but I would really like --

THE COURT: You may have one follow-up and not, well, how many -- what's the percentage of accidents that could happen? Is it three accidents, because there's three different ways to turn it off? You may ask one follow-up question.

BY MR. PRICE:

Q Requiring users -- or if a user had to repeatedly decline the invitation to enable Location History, would it increase the likelihood of enabling it by accident?

A No.

Q Repeatedly asking somebody to turn it on --

THE COURT: I'm going to let him have this. This is just cross-examination, Mr. Simon.

A The reason I say no is the Maps, for example, prompt that you're mentioning, we only triggered it -- I believe that logic was twice per user. If the user either abandoned, didn't respond, we would show it one more time. If the user just missed it, we would never prompt them again.

In each of these, again, the goal is not to spam a user relentlessly. You want this on. You want this on. So we do have controls in place to ensure. And, again, it's very nuanced. It's not -- you know, if you happened to see it but didn't respond, we'll show

you again in a certain period of time. It wouldn't have been the next day. There is logic behind this that would say, depending on the product, don't show the user this prompt again for 10 weeks or however many months, until later.

Then there's also logic that says if you showed the user and the user explicitly said no, do not show the user again.

The logic varies by app and context, but we go out of our way to ensure that we are not doing what you suggest, of just pomeling and pomeling. There is some logic baked in that would stop it. And this is at the account level.

So signing in to a new device would not suddenly restart all of those triggers.

Q Google did realize it was a possibility, though, correct? That's why you sent the reminder email, for example?

A The possibility that someone might turn it on?

Q By accident.

A No. Sorry. I apologize. No. It was the possibility that someone might turn it on and not fully either understand the granularity of the data that's being collected or simply just wouldn't know at that time necessarily, and we wanted to make sure and

reinforce that a user had full visibility into what exactly we were collecting and how that information was being processed.

Q Remind me. When did you start sending those emails a week later?

A The warm welcome notices started in 2017. The warm welcome emails, I'd have to check. I believe, in my declaration, we put a date in for the Timeline monthly emails, which we sent to users every month. So if you turned Location History on in any context, regardless of the surface, we sent you the Timeline email. And I don't recall the exact date, but it's in one of my declarations that said when those emails started.

The warm welcome email, which we added on top of that, I'd have to check to see when we introduced that. It was not -- I can say definitively it was not in 2018.

Q Not in 2018?

A It was not in 2018.

Q Thank you. Once Location History has been enabled, there's an option to pause it; is that correct?

A Yes.

Q But there isn't an option to turn it off; correct?

A We use the language "pause," not "off," that's correct.

Q In a user pauses Location History, does it delete existing data?

A It does not, no.

Q It only halts the collection of future data?

A That is correct, yes.

Q So if a user wanted to revoke consent to use past Location History data, pausing it would not do the trick?

A That is correct, yes.

Q And the process of deleting the historical Location History data is completely separate from the act of pausing Location History; correct?

A That is correct, yes.

Q And as we were talking about earlier, that data may be retained in some anonymized form even if deleted?

A Yes.

Q One last question for you here. If the user deletes the Assistant app after setting it up through this consent flow, Location History stays on; correct?

A Assistant is not an app in this context. It was not an app in this time frame. So I don't believe there's a process to delete Assistant. But if a user

were to stop using Assistant, Location History would still be enabled, yes.

Q And Google would continue to collect Location History data even if the user stopped using Assistant completely or attempted to get it off his phone?

A Yes.

MR. PRICE: No further questions. Thank you.

THE COURT: I have some questions, and I'll allow you to address them on redirect, but I'm going to ask them before the government starts because that will be more efficient. All right? So you may have a seat. Thank you, Mr. Price.

MR. PRICE: Thank you, Your Honor.

THE COURT: I just want to understand, generally, Mr. McGriff, a couple of things. And maybe you know the answer and maybe you don't. Either way it's fine.

So if Location History, say, is paused and then reactivated, is the data that was collected or retained during the pause time put back into Location History database? So, like, if you had a timeline, and I'm talking about 2018, about this time, if you had a timeline, would it be a blank or would it dump back in?

THE WITNESS: It would be a blank. When you

pause Location History, our collection is fully paused at that time immediately. So there would be no information until you resume the service.

THE COURT: Right. So --

THE WITNESS: It would be a blank.

THE COURT: It would be a blank. It might be in the Sensorvault some way anonymized?

THE WITNESS: There's no collection whatsoever in Sensorvault during the time that the control is paused. All of the data in Sensorvault is exclusively collected in the context of Location History. So when you pause the setting, we stop all collection, and there's no additional storage in Sensorvault for that period. So you would have a blank until collection resumed.

THE COURT: Not even anonymized?

THE WITNESS: Anonymized here is a bit of a red herring. Because this was -- that's a general privacy policy for the company. In the context of us -- sorry. In the context of Location History, there would be no collection in any capacity in any way if the control is paused.

THE COURT: So when you hit the control, it stops the passive collection like when your phone -- it stops it all?

THE WITNESS: Any location collection in the context of Location History is completely stopped.

THE COURT: And it's not reaccessed ever?

THE WITNESS: It is not, no.

THE COURT: So this is a weird question, but Google tracks a lot of data. Do you track how many people actually read the privacy policy, like how long the window is open? And, you know, I'm just saying because I think most people don't, but I'm wondering if -- that's not evidence, obviously, and I'll take whatever evidence I have. But Google tracks a lot of stuff, so I'm wondering if you track when the window is up or if you know how many people actually read it.

THE WITNESS: I don't know. There are teams, not my team specifically, that look very broadly on the best way to present the flows. And they look at any number of signals, including user research, to understand how much of these flows users embrace.

I can say based on that research, again, not done directly by my team, we have even further refined since this flow. There have been now two iterations of a presentation based on that feedback.

The latest flow, for example, if you were to attempt to opt in to Location History through one of these products, we no longer even do full screen

because of feedback that it takes users out of context. So we now have what we call the bottom sheet where the same copy and messaging appears, but it comes up from the bottom. So the user can see above the context where they attempted some activity that triggered it, and then the dialogue comes up from the bottom.

That implementation, I believe, is fully rolled out now, but it has been in flight. Again, these iterations are all informed by user research that that central team is doing around what would help users better understand. So this is a constant evolution.

THE COURT: Right. So let's talk about Location History. Like, do you track how many people hit the carrot, the triangle, to go to the bigger screen?

THE WITNESS: Our team does not, no.

THE COURT: Right. So when you're saying there's something that comes from the bottom, would that possibly be something like the Location History context that would come up?

THE WITNESS: Yes. So, now, like, again, this is new UI. It was not at the time of this. The bottom sheet comes up. It shows -- the same copy, I

believe, it shows more of it now. Again, it's all the way to not fully take over the screen, so the user stays in context. Like you were just attempting to view historical places in Maps, but you don't have Location History on. So where before, and I believe it's in these exhibits, you would have seen a screen, a full splash, Hey, turn it on.

We now leave you in the context, You were attempting to do this, but here is where -- and there's still a carrot there, I believe -- I will have to check -- where a user can view more. But, yeah, that's the expansion.

And then, again, the evolution here is now if a user did say yes in that context, then seven days later we also, in addition to the notification, send the email saying, By the way, this happened. That kind of a change.

THE COURT: Okay. So when you turn Location History off, nothing is collected even to target ads; is that right?

THE WITNESS: Any ads measurement powered by Location History is -- there's no new data for that account available because we've stopped collection.

THE COURT: Okay. And so if you turn Location History off, it also goes off in, like, Web &

App Activity? Does it go off all the way?

THE WITNESS: So, there's location services for the device completely unaffected by a user's decision with Location History. Location History is the only store of precise device location.

What Web & App Activity is storing now is only course and location. So if I attempt some activity or a service with Google, and I have opted in to Web & App Activity, they would know that I attempted that activity in Richmond. And the team is looking -- they coursen the location because they don't need to know that I was in this building in this room for their general purposes. They just need to know that I'm in Richmond.

So Web & App Activity would have some record of, if I opted in, I did or performed some task in Richmond. If Location History -- if it was on for the account, would have more granular information. That I was in this building, would be the likely inference. It would understand that I walked to this building. All the details that are visible in Timeline.

If I turned Location History off, Web & App Activity would still know, if I opted in, that I was in Richmond. So when you mentioned ads, Location History does not power all ads. A lot of the -- any

geotargeting or other use of Location for ads is coming from the location services at the device level.

The specific type of advertising powered by Location History, the store visits that were mentioned, is only possible for users who have opted in to Location History. And so if they turned Location History off, then there's no new information coming in for the account.

THE COURT: All right. So Location Services, can you turn that off, too?

THE WITNESS: Yes. Location Services is the location master for your device. You can just say turn off -- no app or service on my device can have access to my location.

THE COURT: So if you have Location Services and Location History turned off, is Google retaining any data? I mean, in its collection for --

THE WITNESS: We don't have access to any information. And Location Services at the device level supercedes anything else. So if you turned Location Services off, and you have Location History on, Location History is not collecting any information because we don't have access to it.

Location, both IOS and Android, position location master, if you will, as an ultimate control

to say I want this device to have any location awareness or access at all. And then once that's enabled, you get the different options for each IOS. Sorry. Operating system.

THE COURT: So if they're both off, nothing's going in in an anonymized fashion to Sensorvault? I know I'm using, you know, human terms, not Google terms. Not that Google is inhuman. But I do like the Monday morning meetings, by the way. I just have to put that on the record. That's just fabulous.

Okay. So if they're both off, then Google isn't doing this extra service for its customers from your perspective, collecting information from somebody's privacy perspective; correct?

THE WITNESS: That's correct. And also, just to be clear, there's no anonymous collection in Location History. I just want to make that clear.

THE COURT: So none of that goes to the Sensorvault?

THE WITNESS: If Location History is on for your account, everything that's collected is associated with you as a user to that account. And that is to, in part, help us with the full data management of anything collected for you. When you go to Timeline and you view all of your data in Location

History, all of those points are associated with you. If you choose to delete a specific point, date, range, specific visit, we are able to give those controls, because all of that information is associated with you as a user.

What's available in Timeline is a full distillation of everything that has been collected for your account in the context of Location History.

THE COURT: Okay. But there's no process where it gets put into a greater data set?

THE WITNESS: We do use an aggregate. An example would be our COVID mobility reports where we take all of the user's data for a specific area. We aggregate it. We anonymized it. And then we perturb it further by, essentially, adding noise to create a representative model of the aggregate. And we do that to ensure that when we release the mobility reports, saying this was the -- these were the mobility trends in Richmond when the COVID restrictions were implemented versus seven days later, those models are actually not any of our data, even in aggregate. It's a representative model of the trends. And those are what we published in the context of the mobility reports.

This is very similar to what we do with

busyness on Maps. I don't know if you're familiar with the feature. On Maps, if it's a popular place, we'll show you whether or not that place is usually busy at that time.

THE COURT: Oh.

THE WITNESS: But those busyness bars are -- I could delete all of my data. It's not going to change that bar, because the bars there are actually an aggregate. They're not -- it's not even a literal aggregate. It's kind of a sufficiently transformed model that is sufficient for the decision making you're doing when you're looking at Maps. Is it busy or is it not?

THE COURT: Okay. So that's a separate model that happens outside the Sensorvault or --

THE WITNESS: Those models are built off of the data that is within Sensorvault and aggregated. Those are so sufficiently transformed that they no longer resemble user data.

THE COURT: All right. Okay. Now, I'm going to ask a question because this is just lore. If you have geofence or Location History, it's not just doing the ground, right? It's going up? Like it does 3D? So this is my question: If you're doing a search, could you know whether you were on the fifth floor

here or the third floor if you were there for a sufficient period of time?

THE WITNESS: Is that information sometimes available in terms of where we understand a device's positioning to be within a building? Yes. I can't speak to how, if at all, that factors into the warrant process. I would be shocked if they're at the point of being so specific to lore as opposed to area.

THE COURT: So, I can tell you I don't know where I hear these things. I've heard that you could tell whether somebody is in one apartment or another through a geofence.

THE WITNESS: Oh. I can't speak to the warrant process. I can say that data itself, it is possible with -- it is possible at just a raw data level to make some estimation of where a user is -- where a device is in terms of elevation, yes. I don't know how that translates to the --

THE COURT: Right. Well, I would think if you have home Wi-Fi or something, right?

THE WITNESS: There are -- I mean, we've looked at it from several different angles over the years, both in terms of emergency response, someone has a distress, and how we can communicate or how it can be relayed this person is on a specific floor.

Again, all of this comes back to location inference. There are a lot of signals that are available, but they're not always available. So a user may have Wi-Fi enabled; they may not. And so we look at all of those signals and try to infer, to our best estimation, where you are.

This is also true in the context of Maps when you're in a mall. We will do our best to determine whether you are on the second floor of the mall or the first floor of the mall if we have launched our directory to help you navigate indoors. But that's a very nascent area. It's a best guess.

So from my understanding of the warrant process, it's not that granular, and I would kind of be puzzled if they asked us for that, only because we would just say okay. We wouldn't be able to guarantee it in any way.

THE COURT: Right. What it says is it's a meter -- I can't remember the range. Anyhow, I've asked my questions. So you all can follow up on that or not.

I appreciate your putting up with my layperson's terms.

CROSS-EXAMINATION

BY MR. SIMON:

Q Good morning, Mr. McGriff. I'm just going to clarify a number of things with you because I think it would be helpful for all involved.

What is your day-to-day job at Google?

A I am a Product Manager in Geo.

Q Okay. So, in that role, what do you do on sort of a day-to-day basis?

A I look at all of the products and features that I'm responsible for, both what is currently in production, what we are currently implementing to be released into production soon, and then also what we might be working on in the future.

Q And so those products that you have some ownership over, are those, to some extent, quite involved with Location History or how do you determine which products you might have some ownership over?

A It steadily evolves over time. I do have responsibility for Location History overall as a product. As the defense blog posts reference, I also looked at several broader features for Maps, including Maps incognito mode, other general location aware features and functionality. But, again, that is steadily evolving over time.

Q Okay. And in this case, I know you were brought in, in part, because of some discussion about Location History; right?

A That is correct, yes.

Q And you submitted -- we've got a smaller binder that's there and that will be used primarily here. It might go to some defense exhibits. But in that binder, there are a number of exhibits. One's marked Government's Exhibit 3. You can take a look. And we've got Government's Exhibit 3B and Government's Exhibit 3C. Those would be the first declaration, supplemental, and the third.

Are those the declarations that you submitted in this case?

A 3, B, and C, that is correct, yes.

MR. SIMON: Okay. And, Judge, I'd move to admit those as Government's Exhibits 3, 3B and 3C. They've been admitted as defense exhibits, but --

THE COURT: Right. There's no objection, right?

MS. KOENIG: Right.

THE COURT: They'll be admitted.

(Government's Exhibit Nos. 3, 3B, and 3C are admitted into evidence.)

BY MR. SIMON:

Q Now, am I to understand that, as you testify here today, you stand by those declarations; right?
A That is correct, yes.
Q And so your testimony before this Court is merely to clarify through the questions that we ask you; right?
A That is correct, yes.
Q Now, you were asked on direct a number of questions about search warrants, about the geofence. Let's just be clear about it. Your job is not to respond to geofence warrants, is it?
A Thankfully not, no.
Q In fact, you literally -- when Detective Hylton testifies that he served a search warrant on Google for this geofence in this case, you weren't involved in that at all; right.
A No.
Q And you typically don't get involved unless there is some specific sort of technical question about Location History; right?
A That is correct, yes.
Q Okay. Now, because there have been so many questions asked to you about the search warrant, despite it not being your job, I do want to ask you, is it your understanding that a Google geofence

warrant simply calls on Google to provide, based on probable cause determined by a magistrate, a magistrate judge, maybe an Article III judge, to provide only those devices that have coordinates that fall within a certain geofence if Google so determines that they do?

A That is my understanding, that's correct.

Q So the warrant never calls on Google to provide anything outside of the geofence warrant; is that correct?

A That is correct, yes.

Q Not this case in particular.

A That is my understanding, yes.

Q Now, there have been some questions about Location History information, what happened in this case. If the government's warrant asked you to give us those location coordinates, that would be responsive; right?

A Yes.

Q And because Google wants to comply with the warrant as is, it only provides Location History information; right?

A Yes.

Q So in looking at your affidavit -- I'll get the right one up. It's paragraph 16 and 17. It looks like it's 96-1. That's going to be your first

declaration. I'll let you look at those paragraphs, 16 and 17.

THE COURT: This is Government's Exhibit 3?

MR. SIMON: Correct, Judge. My apologies.

A Okay.

Q Now, can you explain -- and also maybe take a look at 21 and 22. Can you explain why -- and they're explained in more detail in 16 and 17 and 21 and 22 of your first declaration, but why don't we have anything other than Location History information returned in this warrant?

A As mentioned, Location History is the precise device storage where you get granular information. WAA would understand, if location was captured in WAA with associated activity, only at a very granular level that you were in Richmond. Or it would depend on if you went to very -- I have family in Halifax, Virginia. There's nothing in Halifax, Virginia. If I go there, I will probably be coursened at a WAA level to being in greater Danville.

THE COURT: WAA is Web & App Activity?

THE WITNESS: Yes, Web & App Activity.

A There are not enough people there. So it's just coursened to a level where they can guarantee a certain amount of privacy.

So these other stores would not have the information that Location History has in terms of the level of detail.

Q Okay. And that's the same with Google Location Accuracy?

A Google Location Accuracy moves even farther in the opposite direction. That collection from the time of collection is anonymized. So it's not associated with a specific user.

Q Okay. And so the bottom line, the reality of why Google returned Location History information in this case is because it's the only thing responsive to a warrant for coordinates that are within a certain radius at a certain time; right?

A That is my understanding, yes.

Q Now, talking about Google location information, we'll get into sort of the business and how Google does its business with location. But the 68 percent confidence interval, when we talk about that, to be clear, we're not talking about that broader 150-meter geofence that we draw; right? That's not where the 68 percent is sort of focused on; right?

A Yes.

Q So it's actually focused on what we're looking at as sort of the display radius; right?

A That's correct, yes.
Q So when we talk about 68 percent, we're talking about 68 percent within the blue radius?
A That is correct, yes.
Q Not the geofence that we draw saying only give us devices within this area; right?
A Yes.
Q Okay. If you want to clarify, go ahead.
A No, no. Yes. Your questions made me realize earlier questions. The answer is yes.
Q Okay. If we talk about certain points in the data set that we have here, there will be Defense Exhibit 3, I think it is, that's under seal, has a number of different data points for the anonymized reference ID numbers we got at the first phase here, within that geofence radius. And there will be points that will say a Wi-Fi point will be 84 meters. And then within 30 seconds, there's a 387-meter display radius. And that's a Wi-Fi point. Could you explain why that might be?
A All of these readings are from device sensors. There could be any number of reasons why the device sensors connect to different signals or record different signals. I can't offer any specific answers for this case, but it is possible that you get

different readings at different times.
Q Okay. As it relates to the accuracy of Google's location information, you would agree that this isn't a shot in the dark for Google, that Google maintains relatively good location information; right?
A It is not a random number generator, no.
Q And it's -- I guess to get to maybe a clearer point, it is a technologically advanced assessment of whether somebody is within a certain place at a certain time; right?
A It is a good-faith attempt to make an informed decision, yes.
Q And so in one particular sort of point, I guess, in that -- sort of that space, is that Google has made the point that Location History information might even be a little bit better or much better than cell-site location information; right?
A That is likely true, yes.
Q So to the extent that we're talking about the folks being within that blue -- in the blue radius, not the broader geofence, Google's got good information on those devices; right?
A Yes.
Q Now, are Google's privacy policies online?
A Yes, they are.

Q They're publicly accessible, then; right? And so are the terms of service, presumably?
A Yes.
Q And if we were to go on Google today, as defense counsel showed you, we'd find everything Google's ever said about terms of services and privacy policies; right?
A Apparently, yes.
Q And when Google users set up Google accounts, it's my understanding that they would be agreeing to Google's terms of service -- right? -- in the process?
A Yes.
Q And would they also be agreeing to Google's privacy policy?
A I believe so, yes.
Q Now, if I show you -- I think you've looked at it already because it's admitted -- Defense Exhibit -- Defense Exhibit 43A, the redlined privacy policy. I'm not going to spend a ton of time on this.
THE COURT: It'd appreciate it going up on the screen.
MS. KOENIG: Sure.
BY MR. SIMON:
Q When we look at this privacy policy --
MR. SIMON: And, Judge, I'm looking at the

first page. It's marked May 25 on the bottom left.
Q When we read the paragraph that starts "Our privacy explains," what's cut out that it explains?
A I'm sorry. Can you repeat that?
Q What is cut out there? What is sort of marked out, as defense counsel's sort of insinuating that it was taken out of the policy? But what is marked out there?
A Well, there was copy that was there that was refined in some way. So that was replaced with the copy below.
Q Okay. And so in many ways, what's happening is Google is sort of maybe moving things around as opposed to totally deleting them or inserting them?
A What's happening here is, again, as I mentioned yesterday, with any product, you are always making improvements. There are always refinements. There are new technologies, new capabilities, new sensors, new understandings. So these are living documents that will always evolve to reflect the current context. All of the inputs of feedback, both from critics and friends, users, all of that is informing in how you continually improve.
So the crossed-out portions are the way they stood at some previous point. The replaced copy is a -- at

the time a good-faith attempt at better presenting the previous copy.

Q Okay. And if you look with me at page 3, I'll end it here, page 3 and 4, but starting with "Information we collect," we collect from your use of our services. Do you see that?

A Yes.

Q And it then begins to provide a list of services that were in that December 18 policy; right?

A Yes.

Q December 18, 2017 policy. If you go to the next page, page 4, are you there with me?

A Yes.

Q Is "location information" on that page?

A Yes, it is.

Q So that would mean that location information was set forth -- that you all collected location information December 28th of 2017; right?

A Yes.

Q Okay. Now, in both of these privacy policies, would it be fair to say that Google provides folks with some reasons that third parties might get information on them?

A I believe that is explicitly mentioned, yes.

Q And one of those reasons is a legal reason; right?

That government might come with a search warrant with probable cause; right?

A The government is crafty, yes.

MR. SIMON: Judge, I think at this point I'd move to admit -- the witness has testified that the privacy policy and terms of services are available online. We pulled in Government's Exhibit 5 and 5A -- I don't think the defense will object to this -- but move in the privacy policy effective January 22, 2019, that's Government's Exhibit 5 and 5A, the terms of service modified as of October 25, 2017. We'd move to admit those.

MS. KOENIG: Judge, I don't believe he's presented those exhibits to Mr. McGriff to identify or even recognize. So I think that's the first problem. And the second, I think, is we have to establish relevancy of those. There may be a relevant reason, but those were certainly something that existed afterwards.

MR. SIMON: Judge, we've -- the privacy policy as of January 22 --

MS. KOENIG: I'm sorry. I missed the date. But I think you still need to show him the exhibit.

MR. SIMON: Sure.

BY MR. SIMON:

Q Can you take a look at Government's Exhibits 5 and 5A? Government's Exhibit 5 is long. So I'll let you flip through it.

A Exhibit 5 is the privacy policy as of January 22, 2019, and Exhibit 5A is the terms of service as of October 25, 2017.

MR. PRICE: Judge, we'd now move to admit Government's Exhibit 5 and 5A.

MS. KOENIG: No objection at this point, Your Honor.

THE COURT: All right. They are entered.

(Government's Exhibit Nos. 5 and 5A are admitted into evidence.)

BY MR. SIMON:

Q Mr. McGriff, just to be clear, I know we've asked you about these privacy policies, but the best evidence of Google's privacy policy in terms of service are going to be from the online sources; right?

A That's correct.

Q In this case, the search warrant called for those location coordinates within the radius, and you've noted that only Location History information was responsive to the warrant; right?

A That's correct, yes.

Q And that means that if the defendant's account didn't have Location History enabled, we'd get nothing; right?
A That is correct, yes.
Q And I just want to sort of be emphatic about that. It is not that he turned on Location on his device; right?
A That is correct.
Q And so when I say that, it's not that I get a phone, and I say I want to use where I am at this moment; right?
A That is correct, yes.
Q And neither is it if I turn on Google Maps, and I want realtime location services, I don't want to just put in one address and go to another, just doing that doesn't enable Location History, does it?
A No, that is correct.
Q And so when we talk about Location History, we're talking about that setting that you have said two-thirds of your customers have found the ability to not enable; right?
A That is correct, yes.
Q Okay. And that's in your declaration that approximately one-third have turned it on; right?
A Yes.

Q But even after it's turned on, even after it's turned on, you can delete it?
A Yes.
Q You mention on direct, you said we use the word "pause"; right?
A Yes.
Q Not for deletion, but for turning it off?
A That is correct.
Q And so when it's paused, it is off?
A It is functionally off, yes.
Q Let's be clear about it. When it's paused, there is no record that would be responsive going forward from Google on the defendant's account; right?
A That is correct.
Q So if I had Location History enabled in this case, the robbery, I think, took place May 20, 2019, if I paused that on May 19, 2019, and I still had location on on my device, and I traveled with it the next day, Location History wouldn't know where I traveled on May 20 that next day; right?
A That's correct.
Q And by the same token, the government could come to you with a warrant five times -- as many times as we wanted. We wouldn't get information on May 20, 2019; right?

A That is correct.
Q All right. When we talk about the deletion, you mentioned near immediate deletion; right?
A That is correct, yes.
Q Can you clarify what that means? If I deleted -- and maybe -- if you can. If I deleted my Location History information at 5 p.m. Eastern, would Google turn the information over to the government if they served the warrant the next morning?
A By design, we will return in response to these warrants whatever we have. The deletion process begins immediately. There is some point in that process where the data is not retrievable for this purpose. And the reason it's hard to put an exact point in time on that is we have servers. The data is stored on tapes and servers. It will take time to propagate through the full system before data is deleted from tapes. But I am also certain that we are not getting to the point of retrieving tapes from data centers to respond to the warrant.

So there is some point in that flow where eventually it's no longer accessible by the tools because it's too far along in the deletion propagation. I just -- I don't have a way of putting an exact time on when that happens.

Q So in this case, we -- the robbery happened on May 20, 2019. We came to Google on June 14 of that same year. If the defendant had deleted his Location History information, it wouldn't have been available by that point; right?

A If it was deleted the day after, I don't see how it would be possible for it to still be available, no.

Q But as a general matter, the near immediate deletion, you're saying that happens in realtime?

A The request is initiated right away. Again, it just takes time to propagate down to tapes.

Q Okay. When we've talked -- and pausing means it's obviously turned off. Deletion means it's deleted. And when it's paused, it's paused?

A Yes.

Q I wanted to go through with you the opt-in to Location History process that you've described in multiple of your declarations, both the first and the third, which will be 3 and 3C, if you want to reference them as we go through it.

Google has server side protections -- correct? -- in terms of what information goes into the so-called Sensorvault?

A Yes.

Q So if a user doesn't follow that consent flow,

Google rejects collecting the Location History information; right?

A I would flip it and say that collection is not initiated unless there's been a valid consent, yes.

Q And the defense has shown you a number of -- a number of screenshots. And I'll get to those with you. But the opt-in on this device, I know you don't have the specific user interface, but we have Location History information on this phone. It had to follow a verified consent flow that Google had at that time; right?

A Yes.

Q And that consent flow, as you noted, a verified consent flow would be the same across all applications and devices?

A It's the same consent that was acknowledged in some context, yes.

Q When we talk about the consent flow that you were talking about on direct for Google Assistant and the consent flow generally, there is always a process by which you would have to see what you're consenting to on the page; right?

A There is some reference to -- yes. Yes.

Q And you'd have to scroll down to get to the buttons in question?

THE COURT: The what question?

MR. SIMON: I'm sorry. The buttons.

THE COURT: So, I think, especially at the end of your sentences, which usually include your key aspect of the question, I'm having trouble hearing it.

MR. SIMON: Okay. Apologies, Judge.

THE COURT: That's fine.

BY MR. SIMON:

Q You'd have to go down to the "Turn on" or "No, thanks" buttons before you consented to, in this case, Location History; right?

A In that specific flow, yes.

Q Now, in your supplemental declaration, and I think you stated on the record that you stand by these declarations, you noted that the defense expert was wrong when he said all you had to do to have successfully enabled Location History information was click "Yes, I'm in" on Google Maps; right?

A Yes.

Q At the same time, the screen that the person would be seeing on Google Maps does say that Google periodically stores your location; right?

A Yes.

THE COURT: So, are you moving into evidence 3B?

MR. SIMON: Judge, I think we've already moved in 3B. I moved them all in together, 3A, 3B, and 3C.

THE COURT: Oh, I thought you just did 3A and 3C.

MR. SIMON: No. If I did, I do want to move in 3B.

THE COURT: There's no objection, right?

MS. KOENIG: That's right.

THE COURT: It's in.

BY MR. SIMON:

Q Now, with respect to the Google Assistant opt-in, did you have a chance to previously watch videos that the defense counsel have provided in preparation for this hearing?

A If I remember correctly, I saw two videos, yes.

Q Did you happen to see possibly a "Got To Be Mobile" video?

A I believe so, yes.

Q I'm going to show you what was formerly marked as Defense Exhibit 8.

MR. SIMON: But I've marked it, Judge, for this hearing, Government's Exhibit 12. It's a video, Judge, that I just think will play for about 15 seconds, and then skip to a certain point in the

video.

THE COURT: All right. Is there any objection to the use of this exhibit?

MS. KOENIG: I don't know what the --

MR. SIMON: This is the "Got To Be Mobile" video that you provided to us in preparation for the November hearing that was no longer on the list for this hearing.

But we can play it, Judge.

MS. KOENIG: I think we need to have a couple of questions that are laid. So we had that on our exhibit list. I'll tell the Court that we don't know when that video was made. So if we can lay a foundation about when that was created, that will be helpful.

MR. SIMON: Judge, ample hearsay has been admitted in this hearing, one. I think it's a YouTube video. We can do that through our expert later subject to connection on the date on that. That has a date to it that defense counsel provided to us again. This is how we have the video and that the witness has said he's watched. I'd like to have him watch the video and say he's watched it. And to the extent that --

THE COURT: Was it played in the earlier

hearing?

MS. KOENIG: It wasn't. Your Honor, this video is a video that we had identified as a potential exhibit for the November of 2020 hearing that we had to continue.

All I'm saying, there is a date that is associated with the video, but that is the video creation date, not when the -- that is the video posting date, not when the video was created, necessarily.

THE COURT: All right. Well, I will admit it subject to those objections.

You know, we're establishing a full record here.

MS. KOENIG: Sure. And I appreciate that.

The other thing I'll just note for the Court is that the video skips. I indicate to the Court that we had anticipated potentially introducing this. We just noticed some flaws with this, and I just wanted to bring them to the Court's attention before we watch it.

THE COURT: Okay. Well, that's different than objecting to its entry. Okay. It's entered.

(Government's Exhibit No. 12 is admitted into evidence.)

MR. SIMON: Thank you, Judge. We'll play it.

(Video is played.)

BY MR. SIMON:

Q Mr. McGriff, in this video, is this what we're talking about when we talk about Location History information?

A No.

Q Okay. This is just sort of what you would agree to if you wanted Google Maps to have realtime information?

A Any app, yes.

Q Any app. Okay.

(Video is played.)

Q Is this where if you were going to enable Location History on this phone, a Samsung Galaxy S9, at setup, is this a possible consent flow screen you'd see on Location History?

A This is a possible flow, yes.

Q Okay. Is Location History on the screen by itself?

A It is. As I mentioned previously, the user would be presented with whatever consents were not already agreed to that were required or suggested required in this context. So the only one that was prompted here is Location History, yes.

Q And to get past this page, you'd have to choose -- what are the options there?
A Two options, "No, thanks" or "Yes, I'm in."
Q Okay. And, again, the line down at the bottom reminds the user. It appears that they can go to account -- myaccount.google.com; is that right?
A That's correct, yes.
Q To change those settings?
A Yes.
MR. SIMON: Judge, no further questions on Government's Exhibit 12 at this point.
THE COURT: All right.
BY MR. SIMON:
Q Well, just to reiterate. This is a possible consent flow, as well -- right? -- that the defendant might have encountered in July of 2018?
A That's possible. The screen immediately before is saying, hey, there's Assistant. Do you want this? And this following screen, "Yes."
Q Where Location History stands alone?
A That's correct, yes.
Q Do you have any reason to believe that that's not a Samsung Galaxy S9 Plus?
A I am not an expert on Samsung devices.
Q Understood.

Now, I want to talk about the reality of Google Assistant and sort of the value that it has, to some extent.

THE COURT: The value it has to what?

MR. SIMON: To some extent.

THE COURT: Okay.

BY MR. SIMON:

Q The Google Assistant -- in opting in through Google Assistant doesn't change that to have Location History information. You first, at least, have to turn location settings on a device on; right?

A That's correct.

Q And that's just if I have my phone, again, I need to tell my phone you can get my location. So it wouldn't change that?

A Correct.

Q It doesn't change that I would have to get to a screen like we've just seen in Government's Exhibit 12, or as defense has posited, where you've got a few more options. You'd have to say either, "Yes, I'm in" or "Turn on" or "No, thanks"?

A That's correct.

Q And at the same time you'd also have to make sure that location reporting is on just beyond the device; right? It's, like, the app level setting?

A Location reporting -- the control that is a subsetting of Location History is enabled on the device that you opted in on if it is a mobile device that can be used for Location History. We don't support all form factors. So, for example, you can't opt in to Location History through a TV. But if you were signed into any other devices, it would not enable location reporting on those devices remotely, no.

Q Just to be clear about your testimony on direct, you don't believe that pressing "No, thanks" that's set forth in Defense Exhibit 7, pages 3 and 4, that that would mean you can't use Google Assistant; right?

A That's not my understanding, no.

Q There was some discussion of -- and, obviously, you'd have to turn on the device. And there's the point about signing in to your Google account. So you still -- if I have a phone, and I have Location History enabled, you could actually just sign out of the Google account altogether on a phone; right?

A That's correct.

THE COURT: Wait, wait, wait. What do you mean by that? Sign out --

BY MR. SIMON:

Q So, you can help me explain it. There are -- when

I have a phone, and I set up a phone, if I tie a Google account to the phone, then the phone has my Google account connected to it; right?

A Yes.

Q And I would have to be signed in to that Google account for Location History information to be accessible; right?

A Yes. You can add a Google account -- multiple Google accounts to a device. Just as easily as you can add them, you can remove them. So you can sign in and out of accounts on a device, yes.

Q And those application level options, talking about in your declaration, particularly the third one, I think it's from paragraph 25, where you talk about you could say allow an application to use my location sometimes, deny it, allow it only while I'm -- or allow it all the time. Those options are available on both Android and iPhone?

A Yes, those are the operating system, OS, level controls for app access to location.

Q Okay. And there's a lot of sort of discussion about privacy concerns of Google users. You'd agree that there's a sort of varying level of interest in privacy by different users; right?

A There are varying degrees of privacy

considerations, yes.
Q So there is some discussion that some people are, like, convenience seekers. I've seen that phrase used.
A Yes.
Q And so by that, I don't mind what Google is asking for -- right? -- because what I'm interested in is going from point A to point B, and I want realtime traffic directions; right?
A That is possible, yes.
Q With respect to the two-thirds of folks who have not enabled Location History, your testimony on that one-third piece is that that has been consistent across the time that Location History has been enabled or has been a product; right?
A For the life of the product, yes.
Q How long has it been a product of Google's?
A Many years now.
THE COURT: How many?
THE WITNESS: Many years now. I believe it was made a product in 2015 or 2016.
BY MR. SIMON:
Q So over the course of those -- in this case, by the time you have 2019 -- four years, the number has been roughly the same, a-third of users have enabled

it?
A That's correct.
Q Two-thirds have decided not to collect Location History information?
A That's correct.
Q And, again, the only reason that you had anything to give us under geofence warrant is because Location History was enabled on the defendant's account?
A That is correct, yes.
Q There was some questions on direct about the search that Google does to give us the responsive information. You don't posit -- right? --that you gave us anything other than 19 devices in this case?
A I have no visibility into the processing and servicing of these warrants.
Q Right. So I'm making a mistake there, too, in asking warrant-related questions. But to the extent that Google responds to the warrant, it is always going to be for only the devices that were within a radius at a certain period of time; right?
A That is correct.
Q And is there a possible way in which -- we've talked about sort of the indexing possibly, the grid and location coordinates. Isn't there a way that Google could possibly keep folks who are in Richmond

on a certain side of town -- I'm going to use the right words here -- sort of separate them out in terms of their location coordinates just based off of where they are at a certain period of time?

A Is the question is it possible to refine the scope of the request?

Q To refine the scope -- the manner in which Google goes about getting information inside of its own servers.

A Objectively, yes. This process could be refined and crafted in a number of ways, yes.

Q On the Google side; right?

A On all sides, yes.

Q When we talk about -- but the warrant in this case, specifically, you agree, just asks for folks who Google determines is within a certain radius at a certain period of time; right?

A That's correct.

Q So it would only be our interest in this case, and the government's interest in other cases, to know which devices were at the site of an alleged crime; right?

A That is my understanding, yes.

Q And the manner in which Google undertakes this search, that is not directed by the government; right?

A No.
Q And when I use "search" -- not to cut you off. When I use "search," I'm not using that in the context of sort of the Fourth Amendment. And when you say "searching the database," you're not talking about the issues at hand here; right?
Let me ask it another way: You're not a lawyer; correct?
A Far from it.
Q And I'll just leave it there.
The discussion of anonymized devices and deidentified is a phrase that Google uses; right? The release of data by Google responsive to the request, particularly just focusing on the first stage here, give us the devices within a certain period of time at the site of an alleged crime. That does not give us the name of the individual involved; right?
A That's correct.
Q It does not give us a phone number of the person involved; right?
A That is correct.
Q It doesn't tell us anything other than the location coordinates that are responsive to them being at the site of an alleged crime at the time alleged in the warrant; correct?

A That is correct, yes.
Q The discussions of Google's business model, location information matters to Google's bottom line in terms of money; right?
A I cannot speak to the impact on our bottom line overall as a company.
Q I guess to use a phrase, location information that users provide you can be used as a commodity within the business?
A I would say -- I would generalize that slightly to say that location awareness is a core component of computing broadly in all contexts at this point in time.
Q Okay. Computing broadly --
A Just there are very few products and services beyond Google that don't rely on some location awareness, whether it be to understand whether or not you can view content in a specific area. I mean, there are broad uses of location information generally in terms of just how information technology works today.
Q Okay. In looking at some of sort of the uses that when Google is providing goods and services to its customers and doing so in an effective way, that's a part of Google's business model; right?

A Our goal is to be effective, yes.
Q And I ask that sort of basic question because when we look at --
MR. SIMON: Can we pull up the first affidavit of Mr. McGriff. This is Exhibit 3.
BY MR. SIMON:
Q In paragraph 5, you sort of note that the use of this information sort of allows a user to store and record their movements and travels; right?
A That's correct, yes.
Q And you sort of used that -- this information is used to do, among other things, sort of make -- sort of make different -- give sort of targeted ads that might be of value?
A Location History isn't used for ads targeting.
THE COURT: I'm sorry. What was your answer?
THE WITNESS: Location History is not used for ads targeting. It's specifically used for ads measurement.
THE COURT: For ads --
THE WITNESS: Measurement.
THE COURT: Measurement. Okay.
BY MR. SIMON:
Q And I think that you corrected me there. So the point is location is what is used for those types of

improvements; right?

A That's correct.

Q Bottom line location, not necessarily what's stored as responsive to this search warrant?

A That's correct.

Q But they're both, in a broad sense, location?

A They are all location, yes.

Q But, again, the only thing we get in this case is what's stored in the Sensorvault, and that's only Location History?

A That is correct.

Q In paragraph 14, I'm just going to ask you to read it and sort of explain for us what you're getting at there.

A Let me read the whole thing.

So, this specifically speaks to ads measurement, and what I had previously mentioned in the context of the COVID mobility reports or other sort of aggregated deidentified uses of this information. It's not from an advertisement or advertising perspective. It's not that I specifically, as a user, went to a specific space or place.

The interest in use here is the effectiveness of I as -- not I at all. That some percentage of people saw this and went to this place.

So paragraph 14 is speaking at a very high level to the fact that in its aggregate, anonymized form, this information can be used to measure the effectiveness. And so that's the measurement, ads measurement.

Not -- no way do we share, and never have we shared, explicitly that I went to a specific place with a third party.

Q Understood. But it's used in an aggregated --

A Correct.

Q In stepping to -- because, again, they're different location services. Just the ability to track location is different than what's stored in the Sensorvault as Location History. So I'm going to ask you about just the location services generally.

A Okay.

Q Those are -- those coordinates, not relevant to this particular warrant, but if I use Google Maps, say, on my phone, you all would use the coordinates from Google Maps to improve services or me as a user of Google Maps?

A I don't know what you mean in that context. Location services at the device level, that would be available to Google Maps. So depending on whether you gave Maps access to -- there's those options you

mentioned; always, never, while in use. So if Maps did not have access to location, then it would not have location awareness. If you granted Maps while in use, it would only have access to device location while you were using Maps, meaning Maps was in the foreground. And if you said always, then Maps will have location access even when you're not using Maps.

So in terms of Maps' specific access to location, it would be determined by those permissions and what the user granted.

Q Okay. Let's say a user grants Google information on its location when using Google Maps. Do you use any of that location -- this is different from Location History information, but do you use any of that location to sort of do things like provide realtime traffic updates?

A That's a great question. Traffic updates and understanding, there are any number of signals that inform that. Again, that's an aggregate. So it's not somehow my experience driving from here, three blocks over, is directly going to change what you see on your navigation experience.

But, you know, if several thousand people drove this way and encountered the same issue, that in aggregate would be reflected. That location signal is

one of many signals, yes.

Q Okay. And things sort of like the -- you mentioned the ads, but if I give Google my location, just generally, you would ensure that I might receive more relevant ads based on location; right?

A Are you speaking about a specific app or do you just mean Google generally being location aware?

Q I mean, you can talk about it however you want to, but I understand Google has a lot of products, and so I don't think it's of great value to go product by product. But just in general, the use of location information as provided by users, not the Location History, but just location services reporting to Google, do you all use that in terms of offering better services to customers, and if so, how do you do it?

A So location is very broad. As I mentioned, you have at its coursest level location used to understand are we able to deliver a certain type of content in this area where we understand the user to be. Are we able to -- you know, is the user in an area where we should be providing certain services to begin with? That's location at its most course level.

Then you get down to a still course level, just a granular city understanding. If you were to open

search right now and say "pizza near me" or "baked goods," the search results would be informed by our best understanding at that time of where you are. And that understanding would be directly informed by whatever service -- whatever consented access we have to your location.

So if you had completely turned off all other device signals, we will have at a very course level if you search for "pizza near me," the fact that that request is hitting our server, we will have some concept, but you might see that the pizza results are all over the Richmond region.

If you then enabled -- you can keep going down giving us more access to different controls. You can opt in to Location History on that device and actively be reporting from that device and attempt that exact same query, and we would have a much more refined understanding of when you said "pizza near me," go right outside. There's a place next door.

So there are a lot of layers to the onion, but we will look to -- our responsiveness or what we are presenting to the user will be directly informed by what we have access to in that specific context on that specific device for that account.

Q I wanted to ask some questions, as well, about,

just generally, some of the exhibits that came in --

THE COURT: So, Mr. Simon. I'm sorry to interrupt you, but do you have a while to go on your cross-examination?

MR. SIMON: I don't think a while to go, Judge, but I think 15 more minutes possibly. I was going to ask my co-counsel if they wanted me to touch anything else.

THE COURT: Right. You know, we are now hitting in -- it's almost -- it's 20 of one. We've been sitting here for a while. So we could either let you finish if it's going to be -- but I don't want to lose folks. You know, sugar levels may be high or low or whatever it is.

MR. SIMON: Okay, Judge. I think we can move it along.

THE COURT: Okay. I'm not trying to rush you.

MR. SIMON: No, no, I understand.

BY MR. SIMON:

Q In regards to the functionality of the phone or of a device, when we're talking about, again, the ability to move in realtime and get realtime, like I'm saying traffic updates, that's a location at the device level setting, but also maybe location reporting; right?

A You have -- yes.

THE COURT: So it's location device and Location Reporting, is that what you said, Mr. Simon?

MR. SIMON: Yes, Judge.

A To be clear, Location Reporting is specifically capital L, capital R, is a subsetting of Location History. If you do not have Location History on, you can't enable Location Reporting. Location Reporting and Location History, distinctly separate from location services at the device level.

If location services at the device level are enabled, and you, for example, in your example, I think you were specifically talking about Maps. You would still have the ability to get access to some location awareness to use Maps. You don't use Location History to use Google Maps.

Q And that's the case for, really, any realtime sort of update on movements kind of application; right? Location History is not needed for that?

A It depends on what specifically you're referring to, but, yes, there are a lot of realtime updates that are possible with only current location, yes.

Q With respect to the emails that are sort of, I think, I use the phrase "cherrypicked" from the Arizona litigation that Arizona has with Google. Is

it your testimony -- it's my understanding that your point is that's indicative of an ongoing sort of conversation that Google employees have.

A Google employees have a lot of opinions, yes.

Q And to the extent that they've been entered here, I think it's fair to say that you don't generally agree with those opinions as they've been expressed.

A Google employees have a lot of opinions. I will always listen to Google employees and what they have to say.

Q That worked. But I wanted to also allow you to comment a bit more about Oracle. You mentioned on direct examination that Oracle will give the least favorable view to Google. Can you expand on what you meant by that?

A Everyone has a narrative. Some facts fit more comfortably in a narrative than others. That is certainly everyone's privilege in advancing a narrative.

Q Mr. McGriff, I realize I went over a number of things with you, but I do want to end with sort of, again, the most, in my estimation, sort of the most important pieces of what we've discussed.

Location History is the only information responsive to a geofence search warrant; correct?

A That is correct, yes.
Q And the reason that Google provided only Location History information is because Web & App Activity isn't responsive; right?
A It is no longer responsive, that's correct, yes.
Q And Google Location Accuracy or services, as it was formerly known, is not responsive?
A Not capable of being responsive, yes.
Q And when we say "responsive," we're saying you cannot put devices within a certain period of time within a certain radius sufficiently to turn that over; right?
A It is not possible, that is correct.
Q Okay. And your testimony here today as it relates to Google Assistant is that you're either going to see a consent flow consistent with Location History being on a page with a few other options or Location History being on a page by itself; right?
A Reiterating that I am not the Google Assistant product manager, my understanding of that flow is that it is dynamic, and depending on a user's previous activities and interaction with Google products and services, they would see some variation of that flow if they chose to set up Assistant at that time.
Q After a user enables Location History information,

separate and apart from whether they have location services on, they can delete it; right?

A Yes.

Q Yes?

A Yes.

Q Okay. And near immediate deletion occurs when they seek to delete it; right?

A Yes.

Q And, third, they can pause it; right?

A Yes.

Q And pausing means it is entirely off?

A There is no new collection, that's correct.

MR. SIMON: No further questions, Judge.

THE COURT: All right. I'm going to ask one question. And I'm going to allow you to stand there in case it prompts anything.

If I were to log in to a Google function on someone else's phone, where does that Location History go? Does it go to the phone?

THE WITNESS: If you had previously opted in to Location History for your account, and then you signed in to another person's phone, if you were -- there's a fork there. If on your previous device, you had turned Location History on and were actively reporting for some period of time, and then you

immediately switched and added your account to another device, then that device would start contributing to your Location History. It would not start contributing to -- let's say it was my device and I didn't have Location History on, you would not suddenly enable Location History for my account. The collection on that device would be to your account, not to my account.

THE COURT: Okay. So if I'm on my law clerk's phone, and I log in to my account, say we both have Location History, does the Location History go -- where does it go?

THE WITNESS: For both of you, and you both have opted in to Location History, then for both of you it will be logged in your accounts on our servers.

THE COURT: But if hers is off, then it just goes to me?

THE WITNESS: If she has not opted in to Location History or if she has paused it, then there would be no collection for her account from the information on the device. It would only be to your account.

THE COURT: All right. I'm not sure that's relevant, but I'm doing my best to make sure I have a full record.

I don't want to confuse what you've said. Does that prompt a question?

MR. SIMON: Judge, that was a fine question for me, but I have -- I do have -- I did want to ask about the 68 percent thing, and it's the last question.

THE COURT: That's fine. I'm really not trying to rush you. Some folks sitting just need hope that they're going to stand soon. We've gotten that in their heads, and so everybody can refocus. So do your job. You're fine.

MR. SIMON: Understood, Judge.

BY MR. SIMON:

Q I did want to explore. We talked a little bit earlier about the technological advancement piece. I was asking that in a broad way because I'm not refined in that space, but the GPS points that are returned in the first stage where we say give us everybody who's in the geofence radius, how does Google come up with those points? How does Google assess those points?

A I don't believe there's any assessment in the actual sensor data reported. So when I talk about the evolution of technology, if you're using -- think about the device that you were using -- the mobile device that you were using in 2014 versus the device

that you're using today. Presumably, you've updated your device at least one time maybe. The sensors on your hardware will be immanently better than sensors on older hardware.

So when I talk about improvements in technology, it's in the hardware itself and the sensors themselves. We are not doing any interpretation on what the sensors report. The sensors say, "This device was in this place." And we are recording that. I believe it's mentioned in one of my declarations. It is captured in that suite of things that we collect in the location proto.

And so we are just saying this device said this to me at this time, captured in time, stored on server. There's no editorializing of that raw location point.

Q Okay. And I guess my question is: Do you have an understanding of what goes into creating a GPS point and particularly one that Google would collect?

A Nothing beyond sort of the standard sensor information that's collected there and put into the report.

Q Okay. And what's the standard sensor information?

A We're looking at -- I mean, it's the triangulation of where we have -- you need to be somewhere where you can actually triangulate on at least three satellites.

So the device needs to be somewhere where you can bounce off of three satellites, and they can say, "Based on these three readings, you are likely here."

To my understanding, that is the extent of the limitation of GPS being captured.

Q And what about in terms of Google's Wi-Fi collection, Wi-Fi point collection?

A If Wi-Fi scans are happening, they are yet another signal that is captured. In terms of the raw point, it is, again, just another piece of information.

Q Okay. And no -- does Google sort of assess anything about their Wi-Fi point accuracy?

A It's difficult to build a house on a potentially moving foundation. So you could move all of these access points tomorrow, and then your device might think something's different.

I don't know if you've had this experience. In San Francisco, if you use BART, the BART station in downtown San Francisco happens to think it's in Oakland. So if you open your phone there and say, "I want an Uber," it will think you're in Oakland. That's just how they've assigned and how they're handling data through their Wi-Fi network. So those are possible, but we don't make any -- I don't have any statements on the quality or how that might shift.

Q But Google -- I guess the assessment by Google of the Wi-Fi access points is in that display radius. The assessment of the Wi-Fi points is in the display radius, and, as you testified earlier, that 68 percent goes to whether they're inside that display radius?
A That's correct.
Q All right.

MR. SIMON: No further questions, Judge.

THE COURT: All right.

MS. KOENIG: Your Honor, I have a pretty short redirect, and so I think no more than 10 minutes. And so if that gives everybody enough hope --

THE COURT: I'm telling you, like, my court reporter is -- it's just too much.

MS. KOENIG: Okay.

THE COURT: I appreciate your effort, but I usually try to keep it at an hour and a half or two, and that's largely because of the sort of focus that certainly Ms. Daffron has, but also a witness could use a break. So I appreciate your effort, but I think we are going to take a lunch break.

MS. KOENIG: Okay.

THE COURT: All right. So we're now at almost one. Can we do 1:30? Does that give people

enough time?

MR. SIMON: That works, Judge.

THE COURT: All right. So, I'm going to tell you that I actually don't know the status now, but as we were beginning to speak, we have learned that AT&T had opened a ticket to the problem, and it's on their end. And they did not have a time frame for resolution. So we may know more now, but I'm not going to ask. We'll update you as we come back in. So I think we certainly made the right call.

I do want us to be cognizant of time. We still have witnesses to go. And so I really am going to ask you all to -- we spent a lot of time with folks, and I want the questioning to be crisp and thoughtful. I want you to do your job, but I really wasn't sure we'd go over into today, and that we still have as many witnesses as we do is shocking to me.

So I'm just going to put that bug in your ear, and hope that you are -- now that we have lots of foundation about how Google works and other things, that we just do what we need to do from here on out.

MR. SIMON: Understood, Your Honor.

THE COURT: All right. Mr. McGriff, thank you. You are coming back, apparently, just for 10 minutes or so. So you're still under oath. And I do

appreciate everybody's good efforts. All right? Thank you.

(Luncheon recess taken at 12:53 p.m. until 1:30 p.m.)

THE COURT: All right. So we're continuing our hearing. Do we have any AT&T participants?

THE CLERK: No.

THE COURT: No. All right. Well, hopefully, you were able to speak with your colleagues.

All right. So we're prepared for cross-examination.

Mr. McGriff, are you chilly?

THE WITNESS: Sorry. I was outside earlier.

MS. KOENIG: I think we're on redirect, but it is an adverse redirect.

THE COURT: Oh, adverse redirect.

MS. KOENIG: It feels like a lot of cross today, I will agree.

THE COURT: Yeah, I got distracted.

Do you want us to hang that up for you, sir?

THE WITNESS: No, this will be fine. Thank you.

THE COURT: Okay.

REDIRECT EXAMINATION

BY MS. KOENIG:

Q Good afternoon, Mr. McGriff.

A Hi.

Q I'm Laura Koenig. We met in the hallway outside of court yesterday.

THE COURT: You definitely have to talk into microphone and slowly.

MS. KOENIG: Thank you.

BY MS. KOENIG:

Q I'm Laura Koenig. We met yesterday outside of the courtroom. And I'm one of Mr. Chatrie's attorneys.

I have a question based on the Court's question to you at the end of -- toward the end of Mr. Simon's questions. When the Court asked if Judge Lauck were to put her, if she had a Google account, if she had put it on her law clerk's phone, and both Judge Lauck and her law clerk had enabled Location History in their accounts, would the phone report the device's location in the Location History timeline to both the clerk's account and to Judge Lauck's account?

A There are a few variables, but, to be clear, if the clerk -- the actions of the clerk and the Judge's -- the clerk and Judge's accounts are fully separate as it pertains to Location History. Nothing

that either does impacts the other's account. So anyone adding their account to another device or vice versa does not impact what that specific account has consented to or not.

If both accounts had Location History -- it's irrelevant, but if both accounts had Location History on, and then they were added to the same device, then both accounts would be updated with information as reported from the sensors on that specific device.

Q Okay. So if the law clerk takes the phone independently to her own home, it would indicate on Judge Lauck's timeline in Judge Lauck's Location History timeline that Judge Lauck's account or device that was activated, her Location History would indicate a mark at the law clerk's home?

A Yes. That is one of the reasons why, with varying degrees of success, I try to always be consistent in saying it is where a device is, not necessarily that the person is with the device they are signed into.

Q I appreciate precision. Thank you.

Going back to the questions that Judge Lauck was asking at the end of Mr. Price's question, I want to make sure that I am clear, because there's pause and deletion. So if a user pauses Location History, the data that had previously been -- the Location History

data that had previously been connected and placed in the Sensorvault, pausing Location History does nothing to remove that data from Sensorvault; right?

A That is correct, yes.

Q And, similarly, if I were to delete Location History that had previously been stored in the Sensorvault, that does nothing to change -- that action by itself does nothing to change that my device will continue sending Location History data to Sensorvault?

A If Location History is on for the account and a user goes and deletes all or some subset of the data collected for that account, it will not impact the fact that Location History is on for the account. The user would have to explicitly turn Location History off for the account.

Q And so, therefore, it would continue moving forward past that deletion point collecting the data; right?

A That is correct, yes.

Q Okay. Government's Exhibit 12, which was that video that we had a little discussion about, do you remember that video?

A I do.

Q At the beginning of that video, I think a matter

of seconds into that video, there was a terms and conditions screen. Do you remember seeing that?

A I do, yes.

Q And that terms and conditions screen, that was Samsung's terms and conditions; right?

A I believe so, yes.

Q Okay. In terms of the privacy policies that we've been looking at on the website versions, those are the complete privacy policies that Google sets forth on their website; right?

A Those are our published privacy policies, yes.

Q And when a user activates a cell phone, do they get an abbreviated version of the privacy policy when they go through the process of setup?

A I don't actually know and certainly can't speak to the broader ecosystem of products and services where a user might create an account or see that.

I can't speak to the format of whether it's a -- of how it's presented. I'm sorry. I wouldn't be able to say anything with certainty about that presentation.

Q So the answer is you don't know?

A I don't know, yeah.

Q When we are talking about the data that is in Sensorvault, this is data that is for worldwide users;

correct?

A If you are able to create a Google account now, you are able to opt in to Location History. We don't collect Location History in every area, but you are able to opt in to the control if you are able to create a Google account.

Q So let's go through. What areas do you not collect Location History from?

A I don't have the exhaustive list in my mind, but they are whatever U.S.-sanctioned countries, I believe. So if you traveled to China, I believe we will not collect for you there. So that's if a U.S. account holder who has opted in to Location History travels to China and, you know, or for some reason we detect that you're in a region where we can't collect, we won't. But I apologize. I rarely look at that list. So I don't know all of the countries that are on that list.

Q Sure. China has a few people in that country; right?

A Yeah.

Q So any person who is living in China and has a Google account, they would not be able to generate Location History on their phone or through their device?

A It gets complicated around all the heuristics that we would use to understand where a user is. So I can -- you know, how do you handle Hong Kong? What do you do if the user connects via VPN and spoofs their location to say they're somewhere else? There are just a host of variables.

We do our best through a set of heuristics to identify where we believe a user is, and in good faith attempt to identify when a user is in a sanctioned area. If we believe on our side that a user is within a sanctioned area, we will stop collection. But, again, some signals are more explicit than others.

A Chinese-based SIM, for example, would be a very strong signal that this is probably a device that should not be collected.

Q Sure. So when we're talking about the two-thirds of active Google users that you're not collecting Location History data on, that includes some of these people -- right? -- that live in countries where you just simply don't collect location data; right?

A If I'm remembering the statement, the statement is that only one-third of the accounts have the control on. So are you -- you're saying of the users who have not enabled Location History for their account --

Q Let's go back and look at the statement.

A Yeah.
Q So if you can turn to your first declaration, which is Exhibit No. 21, and I believe your numerous-tens-of-millions statement is in paragraph 13. So the statement says, in paragraph 13, second sentence, "While a more precise percentage is difficult to calculate, in part due to fluctuating numbers of users, in 2019 roughly one-third of active Google users, i.e., numerous tens of millions of Google users had LH enabled on their accounts."
So when we went back to Mr. Price's questions earlier this --
THE COURT: You just have to be sure we can hear you and you're not going too fast.
MS. KOENIG: Thank you.
BY MS. KOENIG:
Q When we go back to Mr. Price's questions from this morning about how it is that you got to that one-third figure, it appears from what you put in paragraph 13 that you looked at all -- the broader number of Google users in the first sentence; right? You start with the math of how many Google users do we have?
A That's correct. The number of -- specifically, the statement refers to in the way this is usually measured in terms of active Google users. So it's not

simply that there's an account, but it's an actual active account.

Q Sure. Fair enough. Active Google users.

But then when you're looking at the one-third, it indicates it's one-third of active Google users who had enabled Location History on their accounts; right?

A That's correct.

Q But I think what I'm hearing you say, and I want to make sure I'm hearing you right, is that some Google users who are active would not be able to activate Location History simply because of where they are?

A Yes, that is true.

Q Okay. And going back to the question, I think, that Mr. Simon was trying to ask, but I want to make sure I'm clear about the answer again, he asked you, like, would it be possible to segregate data points in the Sensorvault by geographic location. And I believe your answer to that question was yes; right?

A Sensorvault is indexed, as I mentioned -- I don't remember whose question it was. Sensorvault is indexed by Google account. So all of the tools are designed to search and query generally by account. So it is not possible today to say to Sensorvault you can't query by location directly. You have to do it

by account. You need to search each account, and then see within that account do you have any coordinates that fit this area.

Unfortunately, we're not able to search across all the accounts at a high level and say show us all the accounts in this area.

Q So Sensorvault is not segregated by geographic location?

A It is not, no.

Q Sensorvault is also -- the data that is produced in response to a geofence warrant is nothing that -- that that data -- Google would never otherwise produce that type of data from the Sensorvault; right?

A The warrant includes -- when you say "that type of data," what are you --

Q Yeah. That was not a great question. Let me phrase that again. So when you get -- the ultimate result of a geofence data is that at the third stage identifying information from a user's account can be turned over based on the link to the device ID that is stored in Location History; is that right?

A That is correct.

Q And aside from a geofence warrant, you would never otherwise produce that information from the Sensorvault?

A There is no other instance where I'm aware that we do that; that's correct.
Q It's not a practice that Google normally does to produce identifying information through the Location History database?
A That is correct, yes.
Q So it's certainly not at business practice that you have; right?
A That is correct, yes.
Q Okay. You have been the Location History Product Manager since 2016?
A That is correct, yes.
Q And how many people are there on the Location History teams? I'm assuming there are more than one team.
A It is difficult to answer. Do you mean in terms of product managers, software engineers?
Q Let's talk about how many -- how many different kinds of teams do y'all have over at Location History? Probably a few; right?

MR. SIMON: Judge, I think in keeping with the Court's -- I'll use the word "admonition" before we left, I'm going to object as outside the scope. I did, obviously, ask about the emails, but I didn't go into how many people worked with him or was he the top

guy as compared with 15 others under him. I just think it's outside the scope, and we should move on to the next witness, Judge.

MS. KOENIG: Sorry. Actually, Judge, this question is completely unrelated to the emails, but it's more related to -- Mr. Simon was asking some questions about what Google uses Location History for. I'm just trying get a sense of how many employees are dedicated to this Location History project.

THE COURT: All right. I'll allow it.

A Directly in terms of fully dedicated, I believe everyone involved has multiple responsibilities. Fully dedicated, it would be tens. In terms of engineers, yeah, I would say tens.

Q Then there are additional probably tens or dozens of other people who work with you all but are not fully dedicated?

A Well, there are -- as I mentioned when I was asked about my role, I look over Location History, but I also look over a host of other features and products within Maps.

Then you have, for example, there is a marketing team that supports geo as a whole. I don't have a direct marketing need every day, so I don't have a dedicated -- there's no dedicated marketing resource

for our platform. There is a dedicated resource. We just don't call them that -- or that resource has other responsibilities.

Q Sure.

A Similarly, we have a writer that we work with. The writing team works with several teams. So I don't include them in that group of sort of horizontal resources that we leverage that would very much be a part of our team but not fully dedicated to our team.

Q Sure.

A In terms of fully dedicated to our team, the best reference would be software engineers, and we have tens working on this project.

Q Tens with an S at the end; right?

A Tens with an S on the end, yeah.

Q So is it fair to say that Location History is an important project or product for Google?

A I won't feign to know Google's broader prioritizations and where we sit in that stacking. We are certainly one team within the sort of broader scope of location, yes.

Q And it's certainly not Google's goal to diminish the number of users of Location History; right?

A No.

Q In fact, it would be more likely that it is

Google's goal to increase the users of Location History; right?

A That's fair, yes.

Q So let's go back to what Location History does. So Location History tracks where a user's device is; right?

A Yes, for users who opt-in, yes.

Q And it can track a user every hour of the day; right?

A There are a host of variables involved there, but yes, if a user has Location History enabled, we will collect whatever we have -- whatever is accessed from that device.

Q And Location History can actually track a user hundreds of times a day; right?

A Depending on activity, yes.

Q Maybe even thousands of times a day?

A I don't think it would get that high.

Q There are only so many minutes; right?

A Well, there's also the reality if it got that high, there are just general device performance questions and other things, so yeah. There is some upper bound.

Q Fair enough. Location History can track a user even when the user is not actually using the app from

which they enabled Location History. We have gone over that; right?

A It varies by platform, Android versus Apple, but yes.

Q And as we know, unless a -- when a user deletes the past Location History, unless a user affirmatively disables Location History, Google continues to collect the future Location History data points from that device?

A Sorry. I can't parse that.

Q So when a user deletes the past Location History, unless that user goes out on their own and affirmatively disables Location History; right?

A That is correct. Deletion is a separate process from turning on --

Q Let me make this more simple. Let me take out that middle part. So when a user deletes past Location History, Google continues to collect the future Location History from that device; right?

A Yes.

Q Okay. And as we know, I think you've indicated earlier today, Google is going to respond and turn over data in response to search warrants; right?

A It is my understanding that we will respond to any valid request when compelled, yes.

Q Okay. And you said yesterday, and I think even the exact quote you used today or statement you made today was, We are always looking for ways to further improve and clarify how we talk about the product; right?

A All products, yes.

Q But also specifically included in that, Location History; right?

A Yes, including Location History.

Q And so it would be pretty clear if the descriptive text -- right? -- that line that is right below Location History before you hit the drop down arrow, it would be pretty clear if the descriptive text at the opt-in stage said something like, If you enable Location History, you'll be allowing us to track you. You will be allowing us to track you every hour of every day. You will be allowing us to track you even if you're not using this particular Google application. You will be allowing us to continue tracking you if you delete your past Location History. We turn your Location History over to law enforcement when they get a valid warrant. That would make more clear what's happening; right?

A That would provide additional clarity for some, yes.

Q But you're not going to do that; right?
A I respectfully disagree with that suggestion. That is entirely -- the ongoing evolution in any product is to be more clear, be more precise. We are steadily looking for ways to improve all products and services, including Location History. In part, the warm welcome notice, the email, the monthly emails we created, the now yearly summary email that we send, all of those not only tell you what we collect, but give a very visual and clear tangible way.

So it's not just words. Hey, here are a blurb of words that most nonlawyers or privacy-minded people will never read. We actually visualize it and make it very tangible. You went from point A to point B. Here is what we understand those places to be. Here is how we understand you traveled between point A and point B, all with an eye toward making it very human readable and consumable in a tangible way.

Q Sure. And I appreciate that that's the back-end take that you all have done; right? But those emails, that presumes that someone's going to open up something that they might otherwise presume is junk mail; right?
A That is why we have rolled out both notices that were originally tied just to Maps. And to the point

you just made, in this time frame, we expanded to make it an operating system notification. So at the OS level, whether or not you're using a Google product or service, it just appeared Location History is enabled for this account.

And any interaction with that notification, open settings, where very promptly a user would see that is on and be able to turn it off. So it's not just that we had a per product notification. It's not that we simply sent one email. We send monthly emails. We send an annual email. We send an email seven days after opt-in. But in addition, we now also do it at the OS level.

So we've steadily rolled out continued notifications and prompts, and on all of them at the top we prominently feature the controls to disable it if the content that the user sees highlighted there is not what they intended.

Q Sure. But wouldn't the most clear way be to just put all that in the descriptive text, so when the person turns it on, they know exactly what they're getting into at that moment?

A That assumes that every user is reading the descriptive text in detail. What you just read would have been a full page of text, so on most mobile

devices a wall of text appearing.

It's certainly possible. I can't say that you're wrong. But I would say, again, that's a wall of text, and it is not -- I'm not aware of anything that would suggest that users would be more inclined to read a wall of text versus a blurb of text. I'm not aware that anyone has come to the proper exact science that two-thirds of a full screen versus one-third is right.

I think part of this evolution over the years has been: What is the way to reach users where they are? So for the user who doesn't read or expand the carrot, for the user who maybe moves quickly past that but will see the email in seven days, for the user who doesn't see emails but will get an app notification, for the user who dismisses all notifications -- like, you're trying to figure out the best way. There's no slam dunk for any of them would be my opinion.

Q Sure. And it sounds like it's fair to say that you all are very aware at Google that people are not inclined -- users are not inclined to read blocks of text; right?

A Some are, to be quite clear. If they weren't, Location History opt-in would be 100 percent. Some people are reading it. The majority of users are reading it and saying no.

Q Or it's the people that are in China that can't activate it; right? When you're saying the majority of people, you can't assume that the majority of people are making an informed decision to not opt-in. You don't have an evidentiary basis to say that; right?

A I'm sorry. Just so I'm clear, are you suggesting that we -- that Google, as a company, has majority of its users in China?

Q No, no, no. I'm saying that when we are talking about the other two-thirds of Google -- active Google users who have not enabled Location History, you indicated that that feature of the two-thirds includes people who have these devices in countries where they cannot enable Location History; right?

A Anywhere you can create a Google account, you can enable Location History. We may not be able to collect data in that region based on where you travel or any kind of variables, but you can still opt-in on the account level.

The reason for that is I can create a Google account right now on a desktop or my laptop, not connected to a mobile device. I may never attach a mobile device to my account. I still have Location History on for an active Google account.

Q Sure. But then if you are not -- let's say you activate a Google account in China; right? You activate it in the United States. You buy the phone and you're here visiting.

MR. SIMON: Judge, I'm going to object. The witness has testified that Location History --

MS. KOENIG: I'll move on, Your Honor. I'll move on. It's not an important point.

BY MS. KOENIG:

Q But going back to the part you all are very aware that some users, if not many users, will not read blocks of texts; right?

A I disagree with that characterization of my statement. We are aware that there are a wide range of users, different proclivities in terms of what they will and will not do. Our focus is figuring out the way to reach as many users as possible, which is why we steadily refine the tools that we use to reach users.

Some will resonate with some users. Some will not. That's why we continue to refine and evolve. That is what I keep referring to as the further improvements. You never stop. You are always looking at ways you can improve these flows.

Q But at no time in 2018 or 2019 did we have

something as clear as what we decided today, that language that I proposed to you, that was never apparent to a user in the descriptive text; right?

A We never used the copy that you just suggested in any flow that I'm aware of, that is correct.

MS. KOENIG: No further questions, Your Honor.

THE COURT: All right. May this witness be excused?

MS. KOENIG: Yes.

MR. SIMON: From the United States, yes, Judge.

THE COURT: All right. So, Mr. McGriff, I want to thank you very much for your time. You are excused. We appreciate your coming in. You still can't talk to other witnesses certainly about what you've testified to. And, in fact, we should sequester the testimony until this hearing is over. All right? Thank you, sir.

(The witness was excused from the witness stand.)

MS. KOENIG: Your Honor, next the defense calls Sarah Rodriguez.

THE COURT: So that is Sarah Rodriguez, Madam Court Reporter.

MS. KOENIG: I'll have her spell her name. Don't worry.

SARAH RODRIGUEZ, called by the Defendant, first being duly sworn, testified as follows:

THE COURT: Before you sit down, have we cleaned out that area?

MS. KOENIG: I don't believe we have.

THE COURT: So, Ms. Rodriguez, I'm just going to ask you to step aside a little bit so we can apply some disinfectant. Sorry. That's awkward, but I'd rather be safe.

Thank you so much for helping with that.

Ms. Rodriguez, my court reporter can only hear you through the microphone. So you can take your mask off. Obviously, we're cleaning things off. And you have more disinfectant, towels, and hand sanitizer anytime you want to use it. Okay?

THE WITNESS: Thank you.

DIRECT EXAMINATION

BY MS. KOENIG:

Q Good afternoon.

A Good afternoon.

Q You are here today -- oh, please tell us your

name, please.
A Sarah Rodriguez.
Q Can you spell your last name for the record, please.
A R-O-D-R-I-G-U-E-Z.
Q Thank you. And you are here today in response to a defense subpoena; right?
A I believe so. I haven't seen the subpoena myself, but that's what I've been told, yes.
Q Fair enough. And you work at Google; right?
A That's correct.
Q And you just moved into a new position very recently there; right?
A About a month ago, that's correct.
Q And so you are currently a Tooling and Programs Lead and Legal Investigation Support?
A That's correct.
THE COURT: A what? What was the first word?
MS. KOENIG: Tooling and Programs Lead.
THE COURT: Tooling?
MS. KOENIG: Tooling.
THE COURT: Okay.
Q Lead and Legal Investigation Support?
A That's correct.
Q And it seems as though you all at Google tend to

refer to Legal Investigation Support as LIS?
A That's correct.
Q And before you were the Tooling and Programs Lead, you were a Team Lead -- right? -- for Legal Investigation Support?
A Correct.
Q And how long had you done that?
A I had done that for about two and a half years.
Q Maybe three years, one month?
A Correct.
Q And before that you were a legal specialist at Google?
A That's correct.
Q What were your duties as a legal Specialist at Google?
A I worked on a domestic criminal team. And our team processed law enforcement requests for user data coming in the form of subpoenas, court orders, and search warrants.
Q And you graduated from San Francisco State University in 2004?
A That's correct.
Q That was with a Bachelor's of Arts in Liberal Studies?
A Correct.

Q You have not gone to law school; right?
A I have not.
Q And you don't have any other advanced degrees?
A That's correct.
Q So your experience in the legal investigation support team is practical; right?
A Correct.
Q In response to a subpoena to Google that Mr. Chatrie had obtained in 2020, you wrote a declaration; right?
A Correct.
Q In the big binder that is right in front of you, we've got a bunch of tabs in there. Thankfully, you don't get asked about too many of them, I think. But you made a declaration on March 11 of 2020. Does that sound right?
A Correct.
Q And you made that declaration under oath?
A Correct.
Q And if you can turn to tab Defendant's Exhibit 24 --

MS. KOENIG: And Ms. Hancock, if I can have the screen over here activated, that would be helpful.

Q If you'll take a look at that for just a moment. It's Defense Exhibit 24. So it should be -- there we

go. Is that a copy -- is Defense Exhibit 24 a copy of the declaration that you signed on March 11, 2020?

A It appears to be.

MS. KOENIG: And, Your Honor, I move to introduce Defense Exhibit 24.

THE COURT: Any objection?

MR. SIMON: No objection, Judge.

THE COURT: All right. It will be entered.

(Defense Exhibit No. 24 is admitted into evidence.)

BY MS. KOENIG:

Q I want to turn your attention now to your responsibilities when you were at your most recent position at Google as the Team Lead for LIS. Your responsibilities as that Team Lead included processing law enforcement requests directed at Google; right?

A That's correct.

Q And geofence warrants were a part of those law enforcement requests; right?

A That's correct.

Q When did Google begin receiving geofence warrants?

A To my knowledge, I believe our first came in in 2016. I'm not exactly sure when within that year, but that's the first that I was aware that we were receiving those.

Q By June of 2019, how many geofence warrants had Google received?
A I don't know the numbers as of that month, specifically. In 2019, I believe we received around 9,000 total requests for warrants specifically with some subset of that.
Q 9,000 total warrants and a portion of those warrants were geofence warrants?
A 9,000 total geofence requests. So, in some cases, law enforcement isn't aware that they need to submit a warrant. So they may have submitted other lower level legal process to obtain records. So that's included in those 9,000. So, some subset was specific warrants.
Q Okay. And a geofence warrant -- we've talked about this a lot. I'm just going to ask you a couple questions to make sure that you're on the same page as we all are.
A geofence warrant is one that requests all Location History data that Google has for a particular geographic area in a particular time frame; right?
A That's correct.
Q And the warrant does not identify, necessarily, a particular suspect; right?
A Not in a way that Google would typically be able

to process it.
Q So when we're talking about what Google turns over, Google turns over all of the Location History data points within that defined area and defined time frame.
A I'm sorry. Can you say that again?
Q Google turns over all Location History data points that you all calculate fall within that geographic area and that defined time frame; right?
A Correct.
Q And each Location History data point is associated with a device ID number; right?
A Correct.
Q Each data point that comes from that same device will have the same device identification number.
A So the device ID's reference within Location History, yes, I believe that's correct. A user may have multiple devices reporting Location History, in which case that device might be different per user, but per device, that should be accurate, correct.
Q If I have a phone right here, and I'm reporting Location History, my phone has one device ID in the Sensorvault database; right?
A Related to your Google account. So if another Google account is associated with that same device and

is reporting Location History from that device, then that separate Google account may have a different --

Q Thank you for that clarification. I'm sorry. I stepped over the words. Thank you for that clarification.

THE COURT: Ms. Koenig, please slow down.

MS. KOENIG: Okay.

THE COURT: I can barely hear you, which I'm pretty sure means that Ms. Daffron can't type that fast.

MS. KOENIG: Okay. Thank you.

BY MS. KOENIG:

Q Let's turn to Defense Exhibit 3. I'm not going to put it up on the screen. It's something that we have put under seal, but if you can look at Defense Exhibit 3, please.

I'll just tell you that this is the -- what the government produced to the defense as the returns in the Google correspondence that were provided in connection with the returns as it relates to this specific case.

A Okay.

Q So if you turn to page 6 of Exhibit 3, which is just the beginning of the first spreadsheet for the Stage 1 return.

A Okay.
Q In that column, we see the label "device ID"; right?
A Correct.
Q And we just went over that the device ID -- I guess the better way to phrase it would be the device ID is unique to each device as it relates to one account on the device?
A Correct.
Q So, for example, the first device ID that is identified -- I'm on page 6 of Defense Exhibit 3 -- that has five data points that were generated for that device ID; right?
A Yes, that would appear to be the case.
Q And then it goes on to list a bunch of other data points for other device IDs; right?
A Correct.
Q And ID is just an abbreviation for identification?
A Right. And specifically within this Location History realm. So these device IDs are not identifiers for any other specific Google account. It's not cross-referenced outside of Location History.
Q Sure. And that's a point I want to talk about with you. So within Location History, if I have my cell phone here, I have just one Google account that's

associated with that phone. That is my phone's device ID as it resides in the Location History database; right?

A In the context of Location History, yes, this device ID that's listed here is the one that's related to your Google account and the device that's reporting that data and stored within your Google account.

Q And so if, let's say, the Chesterfield County Police Department gets more than one -- I'm pointing at them because that's who this law enforcement agency is. If they get more than one geofence warrant, and my device ID number for that cell phone is swept up in a warrant, warrant No. 1, and it gets swept up in a second warrant, if that same device ID number shows up, it's the same device attached to that one account; right?

A To my knowledge, that would be the case. I'm not -- our team isn't responsible for defining these device identifiers. So if there's any sort of collisions on the actual side that we pull the data from, I wouldn't be aware of that.

Q But you have no information to the contrary; right?

A Correct.

Q Okay. So, in response to geofence warrants

generally, Google developed a process for handling such warrants; right?

A Correct.

Q And Google requires as a part of that process that the geofence warrant have a defined geographical area; right?

A Correct.

Q Is there a geographical area that Google considers too big?

A Not generally. It's very contextual to each individual warrant that we review. So it would be determined based on that specialist who's handling the warrant to review, and then coordinate with our legal counsel to determine if it's a warrant that we need to have sort of a conversation with the law enforcement agent that had submitted it.

Q Okay. So, are there parameters -- and if -- let's -- so it sounds like there is a process; right? The warrant comes in to a Google specialist; right? You have to say yes or no. I see you shaking your head, but we have to make a record.

A Sorry. Yes. So it would come into our system, and then a specialist would pick that warrant up to start processing it.

Q And it's up to the specialist to decide if it

seems too big, like, the geographic area is too big?
A It's up to the specialist to determine if it needs further review by our counsel team.
Q If the specialist thinks, eh, this just looks too big, they go to the lawyers; right?
A They'll take it to the lawyers. There may be an intermediate step where they engage with a law enforcement officer to collect more information about the investigation itself to provide that context in our consult with legal counsel.
Q So that process happens -- that back and forth process happens between Google and its various employees and counsel and with the law enforcement officer; right?
A That's correct.
Q So Google also -- when did Google create this three-step process?
A I believe there was discussion around it in 2018. And the discussion also involved agencies within law enforcement. So our, like, CCIPS is an agency that works -- that we often engage with -- not us specifically, but our counsel engages with to discuss sort of certain procedures that may be relevant for the way that we -- that Google will need to handle these types of requests, especially with reverse

Location History being a relatively new type of request that Google has started to receive.

THE COURT: So, Ms. Rodriguez, I'm going to ask you to say the words of the agency that you just gave the initials for so our court reporter can get it on the record.

THE WITNESS: I'm not sure what it stands for exactly. So I know it's computer crimes, but it's a federal agency that is related to the handling of those types of requests.

THE COURT: And the full acronym is?

THE WITNESS: CCIPS, C-C-I-P-S.

THE COURT: I'm sorry?

THE WITNESS: C-C-I-P-S.

THE COURT: Okay. Thank you.

BY MS. KOENIG:

Q Do you know when in 2018 that that policy was developed?

A I don't know exactly.

Q Has that policy changed over time?

A Yes. In the early days, we didn't have a policy set forth. So there was a very, you know, sort of extended processing and engagement with our counsel team on the legal investigation side engaging with our law enforcement and information security counsel team

to guide us through how we should be engaging with these types of requests.

Q How many warrants has Google objected to because the geographical area was too big as it was listed in the warrant?

A I don't know that.

Q So Google also requires that the geofence warrant have a defined time frame; right?

A Correct.

Q And is there a time frame that Google considers to be too long?

A No. Again, it would be, you know, based on the context of the warrant itself in conjunction with the actual area of the geofence as well.

Q Would you go through that same process that if the warrant comes in, the legal specialist gets it; right? You've got to say yes. I'm sorry. I see that you nodded your head.

A That's correct.

Q And if the specialist says, eh, I just think this is too long, then they'll go to the lawyers again?

A It would be the same process. They may collect information from law enforcement to provide context in their conversations with counsel, and then they would further discuss with counsel what the appropriate

action would be.
Q So that same back and forth between Google and the law enforcement agent; right?
A Correct.
THE COURT: That's a yes, right?
THE WITNESS: Correct, yes.
BY MS. KOENIG:
Q And, again, how many warrants has Google objected to because the time frame was too long?
A I don't know that.
Q Are there geofence warrants that Google considers too sensitive, say, like, politically to comply?
A Not as a policy. Again, it would be contextual based on circumstances that are included in the search warrant itself or that we may be aware of because it's a very public sort of circumstance that we are -- you know, know external to Google.
Q And so are you aware of any examples where Google has refused to comply because it was too sensitive?
A No examples where we've refused to comply, no.
Q Is there a policy about that or is that simple the back and forth that we have talked about?
A It would be the back and forth. I mean, I think there's not a policy in place, but our specialists know that if there is anything that strikes them as

being, you know, needing more information from our counsel team, then they will escalate directly to our counsel team to have that review.

Q A fair amount of discretion is initially placed with the specialist that receives the warrant; right?

A Correct.

Q All right. So once you have the warrant that has the geographical area and the defined time frame, and you have this back and forth, the first thing that you do is you turn over, at the first stage, all of the Location History data points within the geofence to the law enforcement officer; right?

A That are within the specified time frame on the warrant.

Q And then you wait for the government to come back, and they may ask for additional Location History data points beyond the scope of the initial request?

A Right. So it would be Location History data that was outside of the geofence and outside of the initial time frame.

Q And that's the second step of the process; right?

A Correct.

Q And in the second step, can the government ask for all Location History data points no matter the geographical area?

A So, it would be limited to devices that were identified by their device ID in the Step 1 of the warrant.

Q Okay. Has Google objected to geofence warrants because the geographical area in the second step was too big?

A We aren't applying the geographical area constraint to that. So it's really more the time constraint that's applied.

Q The geographical area means nothing, really, in the second phase; right?

A I mean, it's applicable because it's derived from the Step 1 processing, but in the way that we handle these types of requests, the area at that point is already -- it's already narrowed by the records that were produced in Step 1.

Q Sure. But for any device ID that the data is returned in the second stage, there are no geographical limits for that second stage?

A To my knowledge, no.

Q So that data could come from houses; right?

A I'm not sure I understand the question.

Q The location data points that are returned in the second stage, it could come from houses, as an example; right?

A The phrasing is a little confusing to me. So the location information would come from the device always as reported to us. It could include a path through a house.

Q Let me phrase that a little bit better. The data could indicate that the device in the second stage was in a house, for example; right?

A Sure. We wouldn't know that at the time, because the legal specialist wouldn't review any of the data, the actual content of the data itself, or plot it on a map. So it could include that.

Q That device could be anywhere; right?

A Correct.

Q A place of worship; right?

A Correct.

Q Schools; right?

A Correct.

Q Hospitals?

A Any physical location that could have a device within it.

Q Okay. In the second step, has Google objected to geofence warrants because the time frame that was expanded in the second step was too long?

A Yes. And to qualify, the too long is in relation to what was initially ordered on the warrant. So the

warrant may also include, as in this case, specific parameters, so it was plus or minus 30 minutes.

So if the law enforcement officer had come back and said "I want an hour on either side of the original time frame," that would not be permitted within the context of this warrant.

Q If time frame is listed -- if the expanded time frame is listed in the warrant, are there any times where Google has objected to say that time frame, the expanded time frame in the second stage that's listed in the warrant, is too long?

A In the initial warrant, we may have. I haven't been involved directly with any of those types of objections, but we may have.

Q Would it follow that same process where the specialist would identify this issue, then bring it to the lawyers?

A Correct.

Q And then Google would go back to the law enforcement officer?

A That's correct.

Q And there would be some sort of negotiation between Google and the law enforcement officer?

A There would be a conversation. In many circumstances, if there's an issue with the actual

wording of the language on the warrant itself, it may be -- we may require law enforcement to obtain an amended or a newly-issued warrant that addresses the issue that we have identified in the warrant text.

Q Okay. Thank you.

Is there a time limit on when law enforcement must come back to request the additional Location History data in the second step?

A Yes. So our system does only retain the records for a certain period of time.

Q How long does it retain them for?

A Roughly, 60 days.

Q So from the time that the Stage 1 data is produced, that data stays wherever you put it for 60 days?

A Right. It's sort of depending on the actual processing of the warrant. So there's certain events that trigger whether that data is then collected to actually purge. But, roughly, 60 days after the production of the initial stage of the warrant we would be able to then respond to and produce on the follow-up stages to the warrant.

Q How does Google determine that 60-day limit?

A That's guidance from our legal counsel.

Q Okay. And when did Google create that guidance?

A It's evolved over time. I don't have a specific date or even month. A lot of the evolution has happened since 2018 through this most recent year.
Q Has that guidance changed over time?
A Yes. In conjunction with our tooling, which is what determines whether the data is automatically purged at the time, that it would be, you know, 60 days or so.
Q What do you do if the law enforcement officer comes back and makes the second stage request after the 60-day time frame has past?
A We may ask them to submit a new warrant.
Q Are there any times where you just go run the data again?
A It would be under the close direction of counsel if we were to do sort of a secondary search, basically, which is what that would be for us.
Q But that would be at the discretion of Google?
A At counsel's discretion.
Q Google counsel's discretion; right?
A Correct.
Q Do you know if Google has objected because law enforcement -- well, you've already answered that question. Never mind.
Will Google comply with if the officer comes back

in the second stage and asks for additional Location History beyond the scope of the initial request on all of the device IDs from the Stage 1 return?

A I'm sorry. Can you say that one more time?

Q So, if -- so, Stage 1 -- like in this case -- right? -- we have 19 device IDs that are returned; right? You're shaking your head yes.

A Yes.

Q And in this case, the law enforcement officer Detective Hylton, asked for the Stage 2 information, the expanded data on all 19 devices; right?

A Yes.

Q And so Google seemed to do something; right? Like, explain to us what Google did in response to that.

A So, based on my understanding of the events, one of our specialists who was handling this specific case had reached out to the detective to explain -- the way the language in the warrant reads is that Step 2 is supposed to be narrowed from Step 1. So all 19 devices were produced in Step 1. In order to make Step 2 actually useful in identifying devices that were aligned with the facts of the investigation, which Google doesn't know, the law enforcement officer would need to review those and determine which devices

were relevant to the investigation and submit a request specific to those devices.

Q Okay. So, we'll come back to the specific example in this case, but does that happen in every case that law enforcement comes back from Stage 1 and asks in Stage 2 for expanded data on every device that is listed in Stage 1? Is there always sort of an objection to that by Google?

A Not always, no.

Q When would it not happen?

A If the law enforcement officer had demonstrated a narrowing in their request. So if there were a lower number of devices from Stage 1 to Stage 2, then that would be the only real kind of reflection to Google and to our specialist team that the request from Stage 1 had been narrowed in the Stage 2 request.

Q So Google requires that there be less device IDs requested or there be data requested on fewer device IDs in Stage 2 than in Stage 1?

A I wouldn't say it's necessarily a requirement. It's a signal to us of, you know, following the actual three-stage protocol.

Q So are there times, then, where Google has gotten a request from law enforcement, and the law enforcement officer is requesting the expanded data in

Stage 2 on all devices listed in Stage 1, presuming there's more than one device -- right? -- and you don't object?

A It would likely be a conversation with our counsel team in those circumstances in order to determine if there would be a necessary conversation with law enforcement at that point.

Q So that same process. Specialist has a question, goes to legal counsel at Google; right?

A Correct.

Q Maybe there's a conversation with a law enforcement officer; right?

A Correct.

Q Okay. If it's -- is there any guidance that Google has about how much narrowing has to happen?

A There's guidance from our counsel team, but nothing that's developed as sort of a policy or you must adhere to this in every single circumstance.

Q Is the guidance like in a percentage form, like we want 25 percent less devices? I mean, what does the guidance tell you?

A Not any sort of percentage form. There is still that discretion that the legal specialist has in being able to apply the policies that counsel has provided to us.

Q Do you know how many warrants Google has objected to because the officer requested the expanded data on every device that was listed in Stage 1?
A I don't know that.
Q All right. So then we get to the third step. And once you turn over the data points in the second step, you wait for the government to come back and ask for the identifying information on the account user for the particular device IDs; right?
A Correct.
Q So that information, the identifying information, includes an account user's email address?
A Correct.
Q And it includes, if you have it, a name that's associated with the user account; right?
A Yes.
Q And is there a time limit on that when law enforcement has to come back and request the third step data?
A Right. It would be consistent. Roughly, 60 days.
Q Is it 60 days from the time that the second stage is turned over or is it 60 days from the time of Stage 1?
A From the second stage.
Q So to get from Stage 1 to Stage 3 could be a

matter of 120 days?
A Correct.
Q Again, how did you determine that 60-day limit at Google?
A That's a counsel determination.
Q Has that changed over time?
A That's correct.
Q That it has changed over time?
A Yes.
Q How long has the 60 days been in effect?
A I don't have a specific date of when that was launched.
Q Has it been since 2018?
A It's evolved since 2018, but the 60-day sort of determination, I don't have a date for it.
Q Okay. If law enforcement makes the third stage request outside of the time limit based on Google's policy, the 60-day policy, what do you do?
A So it would be a similar scenario at Stage 2 where we may ask law enforcement to obtain a new warrant in order to produce that information.
Q Are there times where you don't necessarily ask them to go back and get a second warrant?
A At counsel's discretion, yes.
Q Will Google comply if the officer comes back in

the third step and asks for the account user information from all of the device IDs listed in Stage 2?

A I'm sorry. What's the question? Will Google comply with that?

Q Yes.

A Based on the way that we understand guidance from counsel is that once we've produced Stage 3 information, no additional information is to be produced on that warrant.

Q I didn't say that very well. I'm sorry. So if you have, you know, you have a number of device IDs that are listed in Stage 2 data, if the law enforcement officer comes back in the Stage 3 request and requests the account user information for all of the device IDs listed in the second stage, will Google comply with that?

A Possibly. It depends on the warrant and, you know, sort of the circumstances related to that.

Q So, the same back and forth process. The specialist gets the third stage request, does a gut check, goes to counsel; right?

A That's right.

Q And if counsel thinks it's important, you all will engage in further discussion with the law enforcement

officer?
A Correct.
Q Okay. So let's go back to the specific requests in this case. In this particular case, Detective Hylton submitted the geofence warrant to Google on June 20th of 2019?
A Correct.
Q And the warrant was dated for June 14, 2019; right?
A I believe that's the case.
Q You can look at your affidavit, absolutely, or your declaration. That's Defense Exhibit 24.
A That's correct, June 14, 2019.
Q Thank you. And Google provided the Stage 1 return information on June 28th of 2019?
A That's correct.
Q And then the Stage 1 return provided Location History information from 19 devices; right?
A Correct.
Q On July 2, 2019, Detective Hylton emailed Google requesting additional location data beyond the scope of the initial request. So made the second stage request for all 19 devices from the Stage 1 return; right?
A That's correct.

Q And so July 8 of 2019, Detective Hylton leaves two messages for a Google LIS specialist regarding his earlier Stage 2 requests?

A That's correct.

Q And the Google employee called Detective Hylton back that same day; right? July 8th?

A That's correct.

Q And the Google employee had to explain to Detective Hylton the narrowing process; right?

A Correct.

Q In that the warrant required Detective Hylton to narrow the number of devices he was seeking the expanded information for?

A Right.

Q They did that -- the specialist did that because Detective Hylton had not narrowed the devices that he was seeking the information for; right?

A Correct.

MR. SIMON: Judge, I think the characterization of the search warrant would be better and it would be more appropriate for this record if she allowed the witness to, at the very least, see the search warrant, what it reads, and then -- because that is a lot of testifying about -- went outside the scope. I just think it would be good for the witness

to look at that.

THE COURT: Is it in her declaration?

MS. KOENIG: Yes.

THE COURT: It's in the declaration, Mr. Simon.

MR. SIMON: Understood, Judge.

THE COURT: She's already testified to it. So overruled.

BY MS. KOENIG:

Q So the Google employee had to specifically advise Detective Hylton about the narrowing process because he hadn't narrowed the list; right?

A Correct.

Q And in this particular case, was there a specific directive that was given to Detective Hylton about how much he had to narrow it from Stage 1 to Stage 2?

A Not to my knowledge there weren't any indications from the individual that processed the warrant that that was discussed, but I wasn't involved in the call directly.

Q And the Google employee who talked to Detective Hylton also had to advise him about what types of information would be produced in the later stages of the warrant; right?

A Correct.

Q Okay. It didn't seem to Google maybe that Detective Hylton was familiar with the stages of the process that Google had set forth?

A I couldn't characterize what -- that's what my report was thinking at the time.

Q Let's now go to Defense Exhibit 1. You can flip to the beginning of Defense Exhibit 1, and I'll put it on the screen for you, as well.

THE COURT: So, apparently, Mr. Simon, your objection is sustained.

MS. KOENIG: It's getting a little ahead of me, Judge.

BY MS. KOENIG:

Q All right. So this is a warrant that's dated June 14, 2019, from Detective Hylton. Did you review the geofence warrant in this case before preparing your declaration?

A Yes, I did.

Q Did the language -- let's skip to the attachments. If you go to the third page of the document, page 3 says Attachment 1. And then the fourth page says Attachment 2. It's got a page number at the bottom that says 2, but it is the fourth page of Exhibit 1.

So Attachment 2 is the language that describes the three-step process that Google requires in these

geofence warrants; right?
A That's correct.
Q Did this language in this geofence warrant regarding the three-step process that Google designed seem similar to language in other geofence warrants regarding the three-step process?
A It appears similar.
Q At some point did Google generate a template for law enforcement officers to use in seeking the geofence warrants?
A Not to my knowledge. But that was what I was referring to before with the CCIPS sort of engagement in helping to socialize the concept of these types of warrants and the three-step protocol.
Q So were you aware of any guidance that Google helped create with CCIPS to give to law enforcement officers about how to seek these warrants?
A I'm not aware of the crafting of any guidance, just the sort of discussions or engagement.
Q Okay. So let's go back to the first stage of the process.
MS. KOENIG: Actually, just a moment, Judge.
BY MS. KOENIG:
Q Okay. So sometimes there have been times when Google has notified users that their Location History

was swept up in a geofence search; right?
A Correct.
Q Do the LIS specialists -- do you all issue that notification?
A That's correct.
Q How does that happen?
A Do you want me to describe the process?
Q I do, yes.
A So, in reviewing the search warrant, we will look for the appropriate nondisclosure order within the warrant. If none exists, we may engage with law enforcement to let them know that our process is to notify users before disclosing data.

The process is somewhat different in reverse Location History because we don't know the users that we would notify until the third stage. So at that point in time in the processing of a reverse Location History warrant, we would --

THE COURT: A reverse Location History warrant.

THE WITNESS: Sorry about that. I'll try to be a little slower.

A So in the processing of a reverse Location History warrant at Stage 3 where the user would be de-anonymized, we would actually disclosure the

subscriber information for that Google account prior to that production if there is not a nondisclosure order and a law enforcement agent has indicated that they have no objection to Google notifying the users. In this circumstance, our team would prepare a standard form email to send to the users that we would then be disclosing the information related to their account.

Q Okay. I'm going to break that down, because that was a little -- there are several stages of that process. So, first, you talked about if the warrant has a nondisclosure order, what do you mean by that?

A It's possible there's one in this warrant.

Q You can take your time and look at it.

A So I'm not seeing the language just in sort of a cursory review here. Within the warrant, there would typically be an order from the judge indicating that Google is not to disclose to any users associated with the investigation or legal process.

It could also be a secondary legal order from the warrant itself that's specific to the same order from the Court that Google not notify the users related to this legal process.

Q But you don't see that nondisclosure order in this warrant at all?

A Not in this that I have in front of me. Let me just double check.

Q Sure. Take your time.

MR. SIMON: Judge, I can clarify. I think the -- so, in part, and this will be subject to Detective Hylton talking about it, there was a nondisclosure order that was gotten later in the process. And I recognize now that we didn't provide the nondisclosure order. And I'm happy to do that, but that's why it wasn't attached here. It's gotten at a separate time because those have to go through a circuit judge is my understanding. So that's, in part, why there was a delay.

So I'll just note it's not attached to the search warrant.

THE COURT: Well, it might be important to this examination. Is there a way to get a copy of it?

MR. SIMON: Sure. I think we can figure out that pretty quickly, Judge.

MS. KOENIG: How quickly because I'm almost done?

THE COURT: How quickly because she's almost done?

MR. SIMON: Judge, not at this precise moment. I can represent to the Court that it wasn't

something that, in my mind, was really sort of going to the heart of what we were discussing here, and never really crossed my mind as something we needed to turn over. But it also wasn't given to me. So I haven't withheld it. He's mentioned it to me, and it's just my mistake for not getting it and handing it over. But I will represent we have a nondisclosure order. We'll provide it to them and do that.

THE COURT: Well, do you have a sense of how long it was? Was it a day? A couple hours? A week?

DETECTIVE HYLTON: Your Honor, it would have been the day that it was actually submitted to Google. I believe it was June 20.

THE COURT: Well, how do you want to proceed, Ms. Koenig?

MS. KOENIG: I will let them produce it, and we'll talk about it with Detective Hylton, I think.

THE COURT: Okay.

BY MS. KOENIG:

Q When there is a notification -- if there isn't a nondisclosure order, then what was the next phase? Like, what happens? So you wait until the warrant gets to Stage 3, and then you notify all of the users whose information is about to be turned over in Stage 3?

A Right. So, the first step at Stage 3 is evaluating if that nondisclosure order was submitted prior to our processing of that Stage 3 request. If we don't have a nondisclosure order, we do engage with the law enforcement officer, again, in a form email to notify them that, you know, if you are to obtain a nondisclosure order, you may submit it to us, but we won't be able to produce subscriber information at Stage 3 until you provide us with that nondisclosure order or you let us know that you have no objection to Google notifying the user.

So that process happens first. If we receive information that the law enforcement officer has no objection to Google notifying, then we will move on to actually notifying the users that we would be producing their subscriber information in Step 3.

So just those users that were requested by the law enforcement officer at Stage 3.

Q Okay. What does the notice tell the individual whose information is about to be turned over?

A It lets them know that we received legal process associated with their account. Typically provides them seven days to provide us with a court-stamped copy of a motion to quash, intending to, you know, sort of engage within the court system on the search

warrant itself. And we will, therefore, hold production of that subscriber information until they -- either the law enforcement officer agent or the lawyer representing the attorney lets Google know that the motion has been either approved or denied.

Q So in every case where geofence warrant is obtained, you will follow that process unless there's a valid nondisclosure order?

A Correct.

Q Is there any language that you need specifically in the nondisclosure order to consider it valid?

A Basically, there has to be a clear order from the Court that Google is not to notify in regards to this legal process, notify our users in regards to this legal process.

Q When you say "clear order," is that subject to that same kind of back and forth where Google will review it and decide what they think is clear or not?

A It can be. Only -- and it would be with our legal counsel depending -- so if it's within the warrant itself, in some cases we may receive the affidavit, and the affidavit may include a statement from the law enforcement agent indicating basically the statement to the judge asking for a nondisclosure order. And in that circumstance, it's not very clear to Google

whether the judge was also, you know, sort of so ordering that request from the agent.

So in those circumstances, there will be that sort of coordination with our legal counsel to review and determine what the next steps would be.

Q And next steps could include going back to the law enforcement agent; right?

A Correct.

MS. KOENIG: Okay. I have no further questions, Your Honor. Thank you.

THE COURT: I have a question, and I'm going to let you stand there so that -- well, actually, I'll let you address it on whatever it is.

MS. KOENIG: Redirect.

THE COURT: Redirect.

MS. KOENIG: Thank you, Your Honor.

THE COURT: It's odd under the law because you're an adverse witness, normally it's direct.

MS. KOENIG: Your Honor, I will -- I have one more thing. Mr. Gill had provided me a possible explanation of the acronym.

BY MS. KOENIG:

Q Does CCIPS -- does it sound -- is your recollection that it may stand for Computer Crimes and Intellectual Property Section?

A Sounds accurate.

Q Okay.

MS. KOENIG: Thank you.

THE COURT: All right. So, Ms. Rodriguez, do you have any sense of what you, as a Google employee, or what Google would consider realtime information? We're hearing testimony about, you know, getting Maps information in realtime. Do you have any understanding of what realtime means?

THE WITNESS: In this context -- or I guess in the Maps context, no. In my context as a legal specialist, realtime would, for the most part, mean a Title III, like a wiretap or a pen register trap and trace order that my team also processes. But in the context of Location History, we don't have that concept. We don't have the capability of installing sort of a realtime kind of tracking process for Location History data.

THE COURT: So the difference I hear you saying, and correct me if I'm wrong, is that realtime is sort of as it's ongoing. It's not historic.

THE WITNESS: Correct. In the context of how I have been trained and engage with this material, that's my understanding of what realtime would mean for the legal investigations team.

THE COURT: So within, say, you know, an hour period -- I don't know. I don't want to go outside our record, but if there were over 50 points, so just under one per minute, that would not be considered realtime; is that right? I know it's all different time. So I'm not trying to put words in your mouth. So answer as you see fit.

THE WITNESS: Right. From my perspective, all the records that we produce in response to reverse Location History warrants are stored. So it would not be realtime in the context that I understand realtime.

THE COURT: Okay. That's my question.

THE WITNESS: Thank you.

CROSS-EXAMINATION

BY MR. SIMON:

Q Good afternoon, Ms. Rodriguez.

A Good afternoon.

Q The discussions with the Computer Crimes and Intellectual Property Section that have been mentioned, those are discussions between, I presume, Google's lawyers and the folks from CCIPS; right?

A Correct.

Q And as far as you're concerned, those are sort of the -- that's the back and forth that you mentioned, primarily?

A Correct. I have no direct involvement in that. Just awareness of, you know, sort of the fact that discussions are happening at that level.

Q Okay. And I know that it's already been admitted by the defense, but I'll ask you, there's a smaller book in front of you, a binder. And I'll show you what's marked as Government's Exhibit 3A.

A Okay.

Q Do you recognize that as your declaration? I'll give you a second to look at the pages there.

A Yes, it would appear to be.

MR. SIMON: Judge, I'd move to admit Government's Exhibit 3A.

THE COURT: No objection, right?

MS. KOENIG: It's already been admitted, Your Honor. It was admitted --

MR. DUFFEY: As a defense exhibit.

MS. KOENIG: But I have no objection.

THE COURT: No objection. Yes.

(Government's Exhibit No. 3A is admitted into evidence.)

BY MR. SIMON:

Q When we talk about the geofence warrant, I'm just going to sort of go through some of the points that you've made in your declaration. And to the extent

you want to clarify them, feel free.

But the geofence warrant calls for the anonymized, deidentified location coordinates for folks who fall within a certain radius. So for a defined geographic area during a defined time frame; right?

A That's correct.

Q And at the time the focus is the unidentified suspect of that alleged crime; right?

A From law enforcement's perspective?

Q Correct.

A To the extent that they indicate that to us, that would be our understanding.

Q Understood. And when processing geofence warrants, you've said you've seen sort of the period between a few minutes and a few hours?

A Correct.

Q Okay. And the -- that time span's limited to that geographic area until the second stage when you get what you've referred to as contextual -- or will get contextual Location History information?

A Correct.

Q And I will show you what's in front of you as Government's Exhibit 2.

MR. SIMON: And it's not been admitted, Judge, but I'll ask to question from it subject to

connection --

THE COURT: I'm sorry. I'm having trouble.

MR. SIMON: I'll ask for it to be admitted subject to connection to our witness's testimony that this is the warrant. This is Government's Exhibit 2.

THE COURT: All right.

MR. SIMON: I'm going to question from it. Can we bring it up?

BY MR. SIMON:

Q If we look at what's -- there's red page numbering on Government's Exhibit 2. If you look at page 4 with the red numbering as the guide, I want to highlight the second full paragraph, not "for each type," but starting "law enforcement officers."

A Yes.

Q The paragraph that says "law enforcement officers will return a list." I think it's the next one. I'm sorry.

Now, it's your understanding -- right? -- that this is the second stage after you all have returned the first stage of deidentified devices within the geographical area?

A Correct. This would be the second stage.

Q And in looking at -- I'm sorry. It was the second paragraph that was already highlighted. I'm just

jumping around a little bit.

You would agree with me that in the second paragraph, it reads that law enforcement officers will review that first stage; right?

A Correct.

Q And will in an effort to narrow down the list of accounts; right?

A Correct.

Q And law enforcement officers, it reads in the next sentence, will attempt to narrow the list down by reviewing the time stamped location coordinates for each account and comparing against the time -- the known time and location information that is specific to the crime; right?

A Correct.

Q Now, you mentioned on direct -- and we can just leave that up. You mentioned on direct the number of geofence warrants -- geofence requests. About 9,000 in 2019?

A Right. It was around that volume.

Q And when you have the warrants, it's your understanding that a judge has determined that there is probable cause for this information; right?

A That's my understanding.

Q And to the extent that there is going to be any

dispute, it's either going to be Google deciding to quash that or seeking to quash that search warrant; right?

A If there's a dispute as to the validity of the warrant?

Q Yes.

A Google would object to processing that warrant if there were a dispute as to its validity.

Q Then if, like in this instance, you comply with the warrant as mandated by a judge, then a defendant who is arrested in relation to that warrant can seek to dispute its propriety; right?

A I'm not familiar with the steps that would typically come once Google produces the data.

Q Understood. And how many sort of different places have signed off on these warrants in your experience? Has it been limited to certain districts, certain states, or is it broad?

A So, we've received from many agencies within the domestic United States.

Q When you say "many agencies," you mean from many agencies, you've received warrants signed off by judges?

A Correct.

Q Or magistrates?

A Correct.
Q In the case of responding to this warrant, I just want to be clear for the record's sake with you, as well as I was talking with Mr. McGriff. The first stage just calls on Google to give us the anonymized, deidentified location coordinates for devices that were within that radius at that specified time; right?
A Devices that had reported location coordinates within the geofence.
Q Okay. And then Google determines, based on the location information that they have, what is responsive to the warrant; right?
A We would search our system, our Location History storage system, in order to determine what's responsive to the warrant.
Q And we had some discussion about that storage system earlier, but would you agree that it's possible for Google to work within that storage system to index sort of device information according to where the latitude and longitude comes back from?
A I'm not sure I understand the question.
Q Okay. So I think it's in part because I think the concept is a bit foreign to me, too. But this notion of the warrant comes back. Google then responds to the first stage. And by doing that, Google enters the

location coordinates to find out which device IDs were present; right?

A So, for -- so processing Stage 1, we would enter in the coordinates, the geofence coordinates that were provided on the warrant and the time frame, and that conducts a search across all of our Location History in order to identify the actual responsive location coordinates that are stored at the user level. So that would -- I'm not sure if that answers your question.

Q Sure. I think that just the follow-up would be that Google could then sort of -- they could work around the way in which they save that Location History information; right? So I could -- I'm positing that I could save the location information to account for users that were in a certain period at a certain time, even before the government comes back and requests that information; right?

A At Stage 2?

Q I'm just talking generally about the Location History information database, the Sensorvault. That you all could take the information that is stored in there and determine that we're only going to store -- store based off of a certain grid, a location coordinate grid; right? To say that we'll only put

these devices that were here at this time here.
A I think this might be a little bit outside of my domain of knowledge.
THE COURT: I'm going to be honest, Mr. Simon. I found that a little confusing.
MR. SIMON: Understood, Judge. And I think that ultimately Mr. McGriff was probably our best understanding of that issue.
BY MR. SIMON:
Q With respect to the second step, your declaration recognizes that the information that is provided at Step 2 of the warrant is more than just about sort of picking out a suspect; right?
A So the information provided at Step 2, I think this warrant might sort of outline maybe what law enforcement is looking for in terms of comparing the information against the known kind of facts of the case that they're investigating.
Q And I think that sort of brings to the point about sort of the facts of the case.
When the search warrant is submitted to Google through the enforcement database, you only get the attachment that shows the process by which to complete the warrant; right? That's one piece that you get.
A That Google receives?

Q Yes.
A Correct. We receive the legal process as uploaded by the law enforcement agent to the LER system.
Q And you don't receive the affidavit that the law enforcement officer submits to the judge?
A It varies. In some circumstances, the law enforcement agent may also include the affidavit. In some cases, they do not. And it also varies whether it's a requirement to submit the affidavit along with the search warrant.
Q Google didn't receive the affidavit in this case, did it?
A I didn't recall.
Q Okay. When talking about the information at the second step, you note in your declaration that you can do a number of things with contextual information at the second step; right?
A Do a number of things --
Q So, in looking at paragraph 10, in particular, you note that you can -- that using that contextual Location History information at the second stage can allow law enforcement to -- it can assist in eliminating false positives and assist in determining if devices were just moving through possibly?
A Correct. In paragraph 11, mentioning the, you

know, law enforcement in eliminating devices that were not in the target location for a long enough period of time.

Q And at the same time also can sort of assess -- determine whether a certain ID is relevant or not relevant; right?

A Correct.

Q So that's just sort of the broader process of determining how to investigate a case. And that will be contingent upon what facts are relevant to a particular crime; right?

A Right. And Google wouldn't necessarily have any visibility into the actual facts of the investigation.

Q Understood.

THE COURT: I'm just going to be clear. That was Defense Exhibit 3A?

MR. SIMON: I apologies. That was 3A. I probably am referring to them all as 3.

THE COURT: No, I'm not sure there was a number on the record. That's fine.

BY MR. SIMON:

Q And we've had emails in this case. I don't know if you've had a chance to see those emails. Have you seen the emails between Detective Hylton and Google law enforcement?

A I reviewed the materials associated with the processing of the warrant when I wrote my declaration, but I haven't seen anything since.

Q Okay. So when you're asked about the amount of communication between Detective Hylton and Google, you're not directly familiar, but maybe talking to other folks about it?

A Reviewing what we have associated with the processing of the warrant, but -- and in conversation with the individual that processed the warrant directly.

Q Would it surprise you if I told you that after the July 1 email and the July 2 email for the second stage that Detective Hylton had not heard back from Google yet?

A It wouldn't surprise me.

Q Would it surprise you if I told you that Detective Hylton was the one who actually initiated a call with Google on July 8?

A That they spoke to someone after calling Google?

Q Correct. That Detective Hylton was the one who reached out to Google on July 8.

A I do recall that there was a voicemail left for, I believe, one of our counsel team members.

Q So the representation that there was any

information being sent from Google to Detective Hylton prior to July 8, his call on July 8, that's not correct; right?

A Well, I believe the Stage 1 was produced.

Q Sorry. I should rephrase that. There were not any communications from July 1 through July 8 on the side of Google until Detective Hylton called; right?

A Right. As far as I'm aware, there was no conversation until that July 8 with an actual Google representative.

Q And you would agree that with respect to making sense of these geofence warrants, it is important to know all the facts of the case; right?

A It's helpful in many circumstances.

Q So when we talk about things like relevance to an investigation, knowing all of the facts in terms of what you have, whether it be starting with sort of whether the culprit appeared to be talking to other people, that would be relevant; right?

A In the context of this warrant, I'm not sure how relevant it would have been. But in my processing of other warrants, it has been helpful to have an understanding of the facts of the case that law enforcement has.

Q And I just mean it, to be clear, I mean it from

the context of law enforcement looking at these warrants trying to make sense of what information is useful. All those facts are critical to making that determination; right?

A For law enforcement?

Q Correct. To determine what to request at Stage 2 of this warrant.

A I would imagine so, that that would be helpful for them to know.

MR. SIMON: One moment, Judge.

Judge, I have been told how to ask that question about indexing. So I'm going to try it once more, if you don't mind.

BY MR. SIMON:

Q Could Google, to your understanding, index the Location History in the Sensorvault by geographical location instead of by account?

A I honestly don't know. I could guess that it was technically possible, but I don't know what other limitations may be at play because I don't monitor the database or the structure of the database directly.

Q Understood.

THE COURT: Thank you, Mr. Simon.

Ms. Koenig.

MS. KOENIG: Sorry, Ms. Hancock. I will need

one more assist with the --

THE CLERK: You should be good to go.

MS. KOENIG: Okay. Great.

REDIRECT EXAMINATION.

BY MS. KOENIG:

Q All right. Just a few more questions, Ms. Rodriguez.

Let's -- so, Mr. Simon was asking you about what attachments would have been submitted to Google, I think, and I think we can clarify this.

So, as we know, Google requires that there has to be a defined geographical area -- right? -- before they'll process the warrant?

A Correct.

Q And there also has to be a defined time frame; right?

A Correct.

Q Okay. So if you can go back to Defense Exhibit 1 -- I know we're switching back and forth with different numbers for the same exhibits. It's confusing.

So if you look at the first page of Defense Exhibit 1, which at the top says "Affidavit for Search Warrant." In that affidavit, in paragraph 28, that

appears to list out the geographical area; right?
This is page 1 of that exhibit. I'm sorry. I see you flipping back through.
A I don't think I have -- so this starts with Attachment 1 as page 1. And I don't -- in Exhibit 1.
Q Okay. Let me show you what's on the screen. There may have been a page that got flipped around.
THE COURT: It's farther back in Exhibit 1.
MS. KOENIG: Thank you, Your Honor.
THE COURT: It's a little bit out of order, I think.
THE WITNESS: I can look at the screen.
THE COURT: It's the last page in Exhibit 1.
A I think this ends with search warrant inventory in return, and then it goes back to Attachment 1.
Q I am so sorry about that. Well, let's look at the screen. Let's look at the page in Exhibit 1 which is labeled "search warrant" at the top.
A Okay. I do have that.
Q Okay. So, in that page, nowhere on that page does it indicate what is the time frame or the geographical area to be searched; right?
A That's correct.
Q In fact, it says "see attached"; right?
A Correct.

Q Okay. And so following that, we see what's the next page after that. We see what's labeled as "search inventory and return"; right? I'm not indicating you all would have seen that.
A Correct.
Q And then there is the Attachment 1 after that; right?
A Correct.
Q And the Attachment 1 that follows the search warrant itself appears to be identical to Attachment 2 in the same exhibit that is attached to the affidavit in support of the application?
A In the -- what you had shown on the screen before, that representation, that would appear to be the case.
Q In Attachment 1 here, as it is attached to the search warrant, that is the document that indicates the date and the time in the first bullet point; right?
A That's correct.
Q And then on the second page of that, it indicates in the geographical area above the picture with the circle of the geofence what geographical area is to be searched; right?
A That's correct.
Q And the paragraphs between those two items discuss

the process, the three-step process that we've already talked about; right?

A That's correct.

Q And so if all that had been submitted to Google was the page that lists -- that at the top says "search warrant" -- right? -- if that was all that had been submitted, there was no way you would have processed that; right?

A Right. If there weren't -- if it said "see attached," but there weren't any corresponding attachments, then that's correct, we wouldn't be able to process this warrant as is.

Q And if the cover page didn't indicate the geographical area or the time frame; right?

A Correct. If this warrant -- as it currently looks on the screen right now and in the exhibits, if that's all that there was, then Google wouldn't have enough information to process the warrant.

Q Thank you.

When you are processing a warrant, does it matter to Google if it's a judge that issues the geofence warrant versus a person who is a magistrate that's not a lawyer?

A It varies by jurisdiction, as I understand it in my training on the legal investigations team. So we

may accept search warrants signed by magistrates and we would accept search warrants signed by a judge.

Q And so the training -- or you would accept it from a jurisdiction that allows magistrates to issue such warrants; right?

A Correct.

Q And speaking of your training, when we talked about that back and forth process between Google and the law enforcement agent on the different stages of the process, do you all, as LIS employees, do you get training on how to handle those types of issues about when you need to go to legal counsel?

A Correct. We get training. We also have a regular sort of engagement, you know, scheduled on a weekly basis with our law enforcement counsel.

Q And Mr. Simon had asked you about the Stage 1 process, and you had replied that all users have to be searched. And we've been talking about numerous tens of millions. Do you have any idea how many millions we're talking about in terms of what the Stage 1 search is of?

A I don't.

MS. KOENIG: Okay. No further questions, Your Honor. Thank you.

From the defense perspective, she can be

excused from her subpoena, Your Honor.

MR. SIMON: And from the United States, as well, Judge.

THE COURT: All right. Well, Ms. Rodriguez, I want to thank you for coming here and for testifying. You are excused. Until we're done with the proceeding, I would continue to consider you under sequestration. Just don't talk to folks about what you've testified to, even though you're not subject to recall. And you probably could. It just keeps the record cleaner, if you're willing to keep things close. We do appreciate your coming.

THE WITNESS: Understood.

THE COURT: And you are excused.

THE WITNESS: Thank you. Do you want me to sanitize this?

THE COURT: If you don't mind, sir, could you clean it off afterward?

MR. MELTON: Yes, Your Honor.

THE COURT: You're good. Thank you.

THE WITNESS: Thank you.

(The witness was excused from the witness stand.)

THE COURT: In fact, since we're calling a new witness, and it's been almost an hour and a half,

how about we take a 15-minute recess. And so that will be until 3:35. How's that?

MS. KOENIG: Your Honor, the defense has no other witnesses to present at this stage. And I think we will be ready for the next government witness.

THE COURT: All right. Well, that's good to know. Even more reason to take a break. See you in 15 minutes.

(Recess at 3:20 p.m. to 3:44 p.m.)

THE COURT: All right. I understand we talked about some logistics, which is why we're coming back a little late. Do you all have a sense of how much longer we will be going? Can we finish today?

MR. SIMON: Judge, I don't intend to -- and I certainly am happy to keep an eye on the clock, but I don't intend for the direct to be more than 45 minutes or so. I think a lot of it is contingent upon cross in both instances. But there are a handful of topics to cover with each witness.

THE COURT: Right. So 45 minutes each?

MR. SIMON: I think so, Judge.

THE COURT: What do you all think? I'm willing to stay late. Otherwise, I would think it would make sense to bring the second witness in on Monday. We can't go tomorrow because all the

electricity is shut down.

MS. KOENIG: We would prefer to get it done today, if at all possible.

THE COURT: Well, I think if both parties are willing to stay a little late, and I apologize to the inconvenience for the marshals and everybody else. I just think the better part of valor would be to finish. And so I will encourage you all to be efficient while, of course, representing your clients with zeal. So we're ready.

MR. SIMON: Judge, we'd call Special Agent Jeremy D'Errico.

JEREMY D'ERRICO, called by the United States, first being duly sworn, testified as follows:

DIRECT EXAMINATION

BY MR. SIMON:

Q All right. Special Agent D'Errico, can you spell your name for the court reporter, please.

A Yes. My first name is Jeremy, J-E-R-E-M-Y. My last name is D'Errico, D-apostrophe-capital E-R-R-I-C-O.

Q And you are with the Federal Bureau of Investigation; right?

A Yes, I am. I'm a special agent with the FBI.
Q And how long have you been there?
A I've been with the FBI since 2012.
Q Okay. In what role are you currently in there?
A Currently, I'm a special agent. Prior to being a special agent with the FBI, I was a computer scientist with the FBI.
Q And do you have any specialized role there with the FBI?
A I do. I'm part of the cellular analysis survey team. We abbreviate it as CAST. It's a team that is specially trained of about 80 special agents and task force officers stationed across the country specifically trained to conduct historical cell-site analysis.
Q Okay. What other positions have you held while you've been with the FBI?
A When I first became a special agent with the FBI, I was on the cyber squad investigating computer intrusions and other highly technology investigations. Currently, I'm on the violent crime squad where I brought my technology expertise to help use advanced technology in the investigations of violent crime.
Q And in your work with the CAST team, do you undergo any certifications or trainings?

A Yes. As part of the CAST team, we have over -- or I have more than 300 hours of training to be able to certify for the team. And that starts with a basic training, an overview of how to conduct historical cell-site analysis. And then from there, the top students move on to the next class, which is an advanced class in historical cell-site analysis.

From there, the top students, again, get invited to what we call a field training exercise, which is where we discuss more advanced topics as well as add time constraints to our work simulating a command post situation for, say, a fugitive or a child abduction.

From there, again, the top students move into a four-week certification phase where we go through training from the FBI from the cellular carriers, including AT&T, Verizon, Sprint, T-Mobile, and U.S. Cellular, as well as over a week of instruction from the Florida Institute of Technology on how radio frequencies work, and additional practical exercises. And that culminates with a practical exam, which we need to pass in order to complete the certification.

Q All right. Now, as a member of the CAST team, are you called on to assess GPS data points provided by cellular companies and other technology companies?

A Yes, I am.

Q Okay. And same with Wi-Fi points?
A Yes, correct. Generally, any type of location points.
Q Okay. And in the course of your time, have you done that with -- done that assessment with Google location information?
A Yes, I have. I've reviewed over a million lines of Google Location History, whether it be from a geofence or a location history attributed to someone's accounts, as well as conducted what I call observations of Google Location History data in play.
Q Have you personally attempted to assess the accuracy of Google location coordinates?
A Yes, I have. I've taken out equipment several times to drive around, record my actual GPS location with a stand alone device. And then on another device, I've collected all of the Wi-Fi access signals that I could hear, as well as the signal strengths, and I used Google's geolocation API, which takes the information from the Wi-Fi access points and returns to me a location, a latitude and a longitude and a point on the map, as well as a display map radius, just as they do with Location Accuracy on the Google devices.
THE COURT: What's a geolocation API?

THE WITNESS: Geolocation API, API stands for Application Programmer Interface, and it is a way for me to send information to Google, Google to process it, and send me a response.

So I send them the information, and then evaluate the response back. I compare their location that they provided and their maps display radius that I measured with an independent device.

Q Now, have you ever successfully located anyone using Google location information?

A Yes, I have.

Q Can you tell us about that?

A This is information that myself and the CAST team regularly uses in child abductions, in locating fugitives that do not want to be found by law enforcement, and other folks that may have gone missing.

Q Have you been certified as an expert before?

A Yes, I have.

Q In what fields have you been certified?

A Historical cell-site analysis and location data analysis is generally the title we use.

MR. SIMON: Judge, at this point I'd move the Court to declare Special Agent D'Errico an expert in the field of location, data analysis, including

Google's Location History information.

THE COURT: Any objection?

MR. SIMON: No, Your Honor.

THE COURT: Okay.

MR. SIMON: And, Judge, I've handed the exhibit earlier -- the witness the exhibit earlier, as well as defense, Government's Exhibit 6. It's Special Agent D'Errico's C.V., and I move to admit it at this time.

THE COURT: Any objection?

MR. SIMON: No, Your Honor.

THE COURT: All right. It will be admitted as well, and he is certified as an expert.

(Government's Exhibit No. 6 is admitted into evidence.)

BY MR. SIMON:

Q Now, Special Agent D'Errico, have you worked with geofence warrants before?

A Yes, I have.

Q About how many have you worked with?

A Geofence warrants, at least a dozen, probably more.

Q Okay. Now, did Google provide any data under this geofence warrant any different than what they provided to you in the past?

A The records have been consistent with this among the other geofence warrants I have worked.
Q Now, just to -- we've talked about geofence warrants, obviously, for a few days now, but how would you describe a geofence warrant?
A A geofence warrant is when the government obtains a search warrant commanding Google to provide all of the devices that have Location History records within a particular area and within a particular time frame.
Q And in the course of your time assessing Google geofence warrants, have you come to believe that there are certain best practices in terms of putting together a geofence warrant?
A Yes, I have.
Q Okay. And can you tell us some of those best practices particular as relates to a radius?
A Yes, particularly to drawing the geofence, it differs between investigations from investigation to investigation. In the example of a bank robbery, we're looking for a few things. We need to cover the area of the crime, the bank, but we're also looking for areas where the subject may have entered the area or exited the area. We're looking for areas where the suspect may have parked a vehicle, because we know a few things about bank robberies.

(A) They don't always park in the front space in the front of the bank to go in and rob that bank.

(B) We typically see them park a little bit of a distance away, sometimes in the next parking lot.

We also know that Google location records in a normal interval occur approximately every two minutes. So we need to take these calculations into effect when we're drawing a radius or a box for a geofence warrant.

We try not to capture roadways or other areas where many people may be passing through unless it could be relevant to the investigation. Whereas, in a child abduction, we may want to capture a roadway so that we can talk to people that may have seen the child walking across or along the roadway.

So it really varies based on the type of crime and the layout of the crime scene area.

Q Now, did you prepare a report, a presentation, in anticipation of this hearing?

A Yes, I did.

Q I'm going to show you the pages of Government's Exhibit 1 and let you take a look at those. It's in the folder in front of you. Do you see Government's Exhibit 1 there?

A Yes, I do.

Q Is that the presentation that you prepared?

A Yes, it is.

MR. SIMON: All right. We move to admit Government's Exhibit 1. I know it's been questioned on already.

THE COURT: No objection?

MR. PRICE: Your Honor, there is one slide that we anticipate having an objection to.

THE COURT: Okay. Do you want to lay the foundation for it now so it doesn't go on the record?

MR. PRICE: Sure. This would be Slide No. 47.

THE COURT: What is the basis of the objection?

MR. PRICE: Relevance, Your Honor. It's our understanding that this web page and the language on it --

THE COURT: Okay. I'm having trouble with your mask.

MR. PRICE: It's our understanding that this web page and the language on it did not exist until 2020, long after the events in question in this case.

MR. SIMON: Judge, I think my response to that objection to relevance is that we've seen exhibits come in and out of evidence with no regard

for, I think, dates in part because it does offer some context here in terms of what location services and Location History mean to Google. And I think that's certainly more of a weight, particularly at this hearing. So, Judge, I'd ask to leave that slide in in the presentation.

THE COURT: I'm going to make the same ruling I did with respect to much of what you entered in. You can cross-examine about it and argue the weight of it, and present the weight of it, but we're really not in an evidentiary hearing in any event, and I'm trying to keep the record full so that whatever arguments need to be made can be supported and challenged in a complete way. So it's overruled.

MR. PRICE: Thank you, Your Honor.

(Government's Exhibit No. 1 is admitted into evidence.)

BY MR. SIMON:

Q Now, Special Agent D'Errico, I want to talk about -- you heard me earlier, I'm sure, ask witnesses about GPS points and Wi-Fi points. I want to talk about, first, the Slide No. 3 here.

MR. SIMON: And I'm just referring to the page numbers that will be on the bottom right, Judge, of each page.

BY MR. SIMON:

Q Can you explain for us what we're talking about when we talk about a GPS point?

A Yes. The GPS points in the record, and those are points that have a source of GPS, those points are primarily captured using the Global Positioning System. And the Global Positioning System uses a network of satellites that are in orbit around the earth, and they are constantly broadcasting signals.

The phone, the mobile device, needs to hear at least four of those signals in order to determine the latitude, the longitude, the altitude, and the time. And there's information specifically coded into those satellite transmissions, those broadcasts, that allow the device to do that.

Now, in order to get a good fix or a good location with GPS, you need to be able to hear those satellites or the device has to hear those satellites. So GPS does not work very well inside of buildings such as this but works very well outside, and is what we typically rely on for navigation, realtime navigation with a GPS device or turn-by-turn navigation.

Q Now, we didn't just get GPS points in the returns here; right?

A Correct. We also received points that were

primarily derived using Wi-Fi access points, and they're marked as Wi-Fi in the source column.

Q In Slides 4 and 5, do you explain that?

A Yes, I do.

Q Okay. And so looking at sort of Slide 5 -- and we'll bring up both 4 and 5 next to each other. But when we talk about Wi-Fi fingerprinting, can you explain what we're talking about there?

A Yes. On page 5 is an illustration of Wi-Fi fingerprinting, and this is a technique that is used to determine the location of a device using Wi-Fi access points. And Wi-Fi access points are stationed all over, right? So if you are able to access Wi-Fi on your phone, you're within range of a Wi-Fi access point.

Now, the way that fingerprinting works is that there's a two-step method. The first step, which is above the dotted line on page 5, is what we call training data. And this is when we have a phone that can hear access point No. 1, access point No. 2, and access point No. 3, or, in this case N, because it can be more than three access points.

It hears these access points, doesn't necessarily have to connect to those access points, but hears them and can measure the signal strength of them.

Also at the same time, the mobile device is taking a GPS coordinate. So it's actually determining its location with GPS but also collecting the Wi-Fi broadcast in the area. And what happens with this data is it's sent up to Google as part of the Location Accuracy service. And that Location Accuracy service is an opt-in service on Android phones that allows Google to collect the approximate location of Wi-Fi access points.

THE COURT: I'm sorry. Can you use the phrase again? Location what service?

THE WITNESS: Location Accuracy.

THE COURT: Okay.

BY MR. SIMON:

Q In looking at Slide 6, does Google notify individuals that they will be using Wi-Fi access points to assess location devices?

A They do. Can I go back to Slide 5 and finish the bottom?

Q Sure.

A I'm sorry. So, we talked about the training data set up top. The next set comes in on the bottom of that page where a phone does not collect a GPS coordinate, but it does collect the Wi-Fi access points and the signal strengths. It can then send

that information to Google, which collected a database and created a fingerprint, so to speak, and associated the same access points with similar signal strengths to determine an approximate location.

So there's no need to know an exact location for every access point in the world. What we need to know is the access points in relationship to others and approximate signal strengths. Using that information, we are able to efficiently determine a location without using GPS.

And there's occasions where we don't want to use GPS because GPS is very expensive on the battery. We heard Mr. McGriff testify that there might be problems if there were thousands of points, particularly GPS points, from a device. So Wi-Fi is a less expensive but still accurate method of providing the approximate location of a device.

Q Okay.

A Thank you.

Q And to go back to my previous question, is Slide 6 demonstrating Google's notification to customers that it uses Wi-Fi access points to assess location?

A Yes, it does.

THE COURT: You're so far away from the microphone.

MR. SIMON: I apologize.

THE COURT: You're talking to him, but we're the people who need to hear it.

MR. SIMON: No, I understand. And I moved a little bit, so I'll try to maintain --

THE COURT: That's fine.

BY MR. SIMON:

Q So I'm looking at Slide 6. Is that slide demonstrating Google's notification to its customers that they use Wi-Fi points to assess location?

A Yes, there's two places on Google's site that discussions Wi-Fi and the use of it. So in the top block, Google says, To improve location services, Google uses publicly broadcast Wi-Fi data from wireless access points and GPS, cell towers, and sensor data. Only publicly broadcast Wi-Fi information is used to estimate the location of a device.

In a separate article, it also talks about how you can, as a Wi-Fi point owner, opt-out of Google using your Wi-Fi access point in location services.

And on the bottom, Google also talks about their Google location services, otherwise known as Google Location Accuracy. That uses information of nearby Wi-Fi mobile networks and device sensors to improve

its location device or its location data using the Android phone.

Q Okay. Now, I want to show you what we've marked as --

THE COURT: I'm just going to ask a question. You said there's a separate article about how you can turn it off. That's not reflected on this slide; right?

THE WITNESS: Correct, that is not reflected in the slide.

THE COURT: Okay.

BY MR. SIMON:

Q And I just want to now have you look at Government's Exhibit 2.

A Excuse me?

Q Government's Exhibit 2.

A Yes.

Q Do you recognize the pages set forth in Government's Exhibit 2?

A Yes, I do.

Q What is it?

A This is the search warrant and affidavit that Detective Hylton submitted for the Google geofence warrant.

Q Okay. And that's a fair and accurate depiction, I

presume, of that application?
A Yes, it is.
MR. SIMON: Judge, we move to admit Government's Exhibit 2 at this point.
THE COURT: Okay. No objection; correct?
MR. PRICE: No objection, Your Honor.
THE COURT: Okay. It's entered.
(Government's Exhibit No. 2 is admitted into evidence.)
BY MR. SIMON:
Q Now, let me ask you about the geographical area. We've talked about that phrase throughout the few days. What geographical area was deemed relevant to the search warrant in this case, looking at Slides 8 and 9?
A And this is back in Defense Exhibit 1?
Q Defense Exhibit 1, yes.
A So Slide 8 on my report, Defense Exhibit 1, shows a red dot towards the center of the slide with a red circle around that slide. The red dot is the center of that geofence, whereas the red circle illustrates the effective geofence, which is 150 meters away in every direction from that center point.
Q Okay. And so this is the geofence radius we have. Now, did you put slides together to sort of

demonstrate what factual points went into developing that geofence?

A Yes, I did. Slide 9 goes into that point. So it's important for us to capture all areas where somebody could stash a car or hide a car, and also all areas where somebody could arrive or leave from this crime scene.

So, in this case, what was done was the geofence on the right side goes up to but doesn't cover the road, which is Price Club Boulevard, traveling north to south and curving towards the west under the geofence. On the south side of the geofence, that area covers the area behind Journey Christian Church, which is the church where we received information that a suspicious blue Buick was parked, and it also covers the wooded area, because we know that subjects when fleeing a bank robbery may not --

Q Special Agent D'Errico, I'm sorry to interrupt you, but can we look at, while you're explaining this, Slides 10 and 11, because I think some of those points might be in there; right?

A Yes. We also cover the area south because we know subjects may flee through the woods and may not use the road system.

On the left, we cover up to the adjoining

business, which we can see also covers some trails. And then to the north, we try to cover as much of the parking lot as we can but try not to cover the area near the Hampton Inn.

And on Slide 10, we have additional information laid on the map, particularly yellow markers that indicate the approximate location where we saw the subject via surveillance cameras from both Journey Christian Church and from Call Federal Credit Union.

There are two triangles or partial triangles on the maps with the points attached to the side of the church. The one in purple towards the bottom is the field of vision of one of the cameras, one of the surveillance cameras, that we were able to obtain surveillance footage from.

The one towards the top, in orange, is, again, a field of view of a second surveillance camera that we were able to get coverage from or a video from during the time of the robbery.

And then we have video surveillance from the area withinside the Call Federal Credit Union. And each one of those yellow pinpoints indicates a point where I observed the subject on this map.

So we can see that there were video observations that start on the bottom with No. 1 and travel the

parking lot in between the church and the credit union towards the north, and then there's points, specifically points 4, 5, and 6, where the subject moves towards the Call Federal Credit Union.

There's point 7, which is inside Call Federal Credit Union. And then points 8, 9, and 10 show points where the subject was running from the Call Federal Credit Union towards the -- well, out of the field of vision but south back towards where we originally saw him on video.

Q Now, did you assess for your presentation -- and these slides are coming up on the screen as well, if it's easier to see them. Did you assess and compare the geographical area covered by the geofence in this case with what's covered by a cell tower dump?

A Yes, I did.

Q Is that reflected in Slide 13?

A Yes, it is. Slide 13 shows the approximate area of coverage that I would expect to receive if we conducted a tower dump for this crime.

Q Now, before you go into it, just for the record, how would you describe a cell tower dump? What is it?

A A cell tower dump is when we obtain a 2703(d) court order to obtain communication records from the cellular providers that correspond to communications

that happen on a particular cell tower.

And, typically, when we obtain tower dumps, we look to obtain any cell site that would provide coverage to the subject area. In this case, the Call Federal Credit Union.

We know that cell phone towers overlap, and that's what allows us to move seamlessly from one cell tower to the next cell phone tower. So we choose three to make sure we are getting complete coverage or as much coverage as possible of that target area, that subject area.

Q And we heard earlier that cell tower dumps provide phone numbers; is that right?

A That's correct. When the phone companies respond back to the 2703(d) order, they provide the actual phone numbers used in the communication. So they are not anonymized. They are the actual telephone numbers used in that course of the communication.

Q What, if anything, does the government tell a cellular telephone company to do in terms of how they would provide that information? Do we tell them how to go about finding the information from the cell tower?

A No, we don't direct them on how to respond to the Court order other than directing them to provide

records that cover that area.

So my understanding is that they use the processes that they have in order to obtain those records that they use in their ordinary course of business.

Q And what -- you've dealt with both types of warrants, geofence warrants and cell tower dumps, which can come by a subpoena; right?

A A cell tower dump?

Q Yes.

A I've only obtained them with a 2703(d) or a search warrant.

Q The -- but the information that comes from the cell tower dump and the geofence warrant, which one provides more data back?

A Typically, more data is received in the tower dump. It will provide -- yeah, more information typically is from a tower dump. It does depend, but usually it's a tower dump.

Q When I sort of say "information," it's like each phone number that comes out of there belongs to a particular user; right?

A That's correct. We get the actual phone number of the user that was in this area as well as the direction from the tower. So it's not just that they were in that area, but it's the direction from that

tower that we also obtain. So an approximate location for that device.

Q Just for the record, you can subpoena, then, the subscriber information for those phone numbers; right?

A We can. We can use a subpoena to obtain subscriber information or use other databases to attempt to determine the actual -- the person who has it in their hand.

Q Now, we've talked about the various stages of the geofence warrant. Did you go about providing a summary of the records returned in the first stage for your presentation?

A Yes, I did.

Q Okay. I'm going to have you take a look at Slide 17.

THE COURT: I'm going to ask a question before you get there. Looking at Slide 13, the blue area, I presume, is the area where you might get information from a tower dump; is a right?

THE WITNESS: That's correct. And I've estimated that based on all of these towers in the area because we know that towers overlap. So we estimated that the three towers that are inside the blue area would be the towers that would be dumped in response to a tower dump order. And that approximate

coverage area would be approximately the size of that blue outlined area.

THE COURT: So how big is the blue outlined area?

THE WITNESS: I didn't do an area comparison, but on the bottom of the map, Your Honor, there is a scale that indicates that it's 4 kilograms between those two points. So width-wise, Your Honor, I would say at the widest part, and I am just eyeballing this, it may be 7 or 8 kilometers wide at the widest part traveling east to west. And then traveling the area north to south, this area may be about 10 kilometers north to south.

THE COURT: All right.

THE WITNESS: Also on that map is the red circle indicating the size of the geofence.

THE COURT: Right. Okay. Thank you.

BY MR. SIMON:

Q Now, looking at the summary of records from Phase 1 and Slide 17, if we look at the top here, it says, Initial Google Geofence records provided by Google and the first 15 of 209 records. What's meant by the first 15 of 209 records?

A This is just a sample of what the records look like when they come to us from Google. And, actually,

they're not even this pretty. But they contain several columns of information, including a device ID that's going to be unique for the device inside this geofence, the date and the time, the latitude and the longitude providing an approximate location. And I should say the center of the approximate location for the device. The source of the device, which is, my understanding, the primary sensor that was used to obtain this.

In this case, we saw records with GPS or Wi-Fi. There's also records out there in other Geofences that use cellular towers and will be reported under cell.

And then the last column is the map display radius, which is the true area around the center point where Google believes that device may be.

Q Okay. Now, did you -- and let me ask you, you mentioned the map display radius. Whenever we see that, it has the same meaning across these returns; right?

A Correct. That M stands for meters.

Q How would you -- I think you've done it. Would you describe sort of our best understanding of map display radius?

A Map display radius is the area where Google believes that the device is located. So while they

provide us latitude and longitude coordinates, that's not the actual location of where Google believes it is. That's the center of the location where Google believes it is.

If I could, I would draw maps without a center point in it and just a bubble because that's a better representation, but it's hard to get the scale or it's hard to understand how many points are then layered on there.

So in the maps that I have, I'll draw it with the center point as well as the bubble around the display radius, understanding that it's not the point that Google is saying that the device is at, it's inside the bubble where Google is saying that the device is.

Q Okay. Now, looking at Slide 20, did you plot all the points returned in Stage 1 of the warrant?

A Yes, I did.

Q Okay. Is this an indication of those plot points?

A Yes, this is all 209 points for Stage 1 of this search warrant return plotted on the map with both their center coordinates marked by the markers, the red or blue markers, and then the display radiuses associated with each of those points.

Q There was some discussion of the 387-meter radius that one of these points provided. Can you explain

why we had such a large radius for one point and then right before that right there was a smaller radius?

A Yes. So in the records, there are two records that are very close in time. I believe it's within 30 seconds. But more noteable is that they were both Wi-Fi records, and they had the exact same latitude and longitude.

The first record had a display radius of about -- I believe it was 84 meters. So a smaller display radius that was inside the geofence.

The second point, about 30 seconds later, had the same exact center coordinates, but it had a much larger display radius, 387 meters. And in my experience analyzing these records, that's indicative to me that the device is moving, that it's traveling. And for some reason, unknown to me, a new center coordinate was not obtained by that phone. But based on the other sensors in the phone, such as a gyroscope which determines the tilt and the angle of the phone, or the accelerometer, which determines how fast a phone is traveling, Google can use these sensors together and determine that this phone moved, and I'm going to adjust my display radius to account for that movement.

Unfortunately, it's not as simple as just using

the GPS coordinates or just using the Wi-Fi coordinates. There are lots of different sensors that go into these calculations.

Q Now, did you ultimately -- I know you did. You reviewed the warrant in this case; right?

A Yes, I did.

Q And did the warrant call on Google to return any information at that first phase? We're just talking about the first step of the search warrant. Did it call on Google to return any information that it determined fell outside of that geofence radius?

A No, it did not. The first stage asked for information regarding points inside the geofence.

Q Okay. Now, I'm looking at Slide 21. Is this an example of, again, sort of what area is covered by the geofence as opposed to the cell tower radius?

A That's correct. I plotted all of those points that we saw on page 20 in the geofence onto the map that has the outline of the estimated tower dump area.

Q Okay. And with respect to the records that we saw plotted in Slide 20, can we take a look at Slide 22. Is this a fuller summary of those records?

A It is. This is a summary device-by-device that lays out how many records we received for each device, the first time that we received a record or the

earliest record for each device, the latest record for each device, and then we also looked at the smallest display radius, and the largest display radius.

And then I took a look just to see how many of those display radiuses extended beyond the geofence area and then what was the maximum distance beyond that geofence area.

Q When we say "extend beyond," again, we're talking about just that blue radius that might fall a little bit outside the geofence but for which Google has concluded they are inside the geofence?

A Correct. All the center points are within the geofence. And these are the map display radiuses for each of those center points.

Q Okay. In looking at -- you were just testifying about those two points that have, sort of within 30 seconds, a different -- a vastly different Wi-Fi radius point. Is that set forth in the device ID line that ends 4289?

A It does. 702354289.

Q Okay. Now, how many points were provided in that first phase of records returned by Google?

A 209.

Q How many of those points belong to the defendant? And can you state for the record which of these

accounts on page 22 belongs to the defendant?
A Yes. The defendant is the device ID second from the bottom. It's 1716665659. And the records -- we received 38 records for that device beginning at 4:20 p.m. and ending at 4:54 p.m.
Q Okay. And if I'm looking here, it appears we don't have the header of each of these columns, but is it right that only one of his points have any radius that extends at any point? The bubble might go a little bit outside of the geofence?
A That's correct. There was one Wi-Fi point that would extend 26 meters outside the radius. And that's the equivalent to a few parking spaces.
Q Okay. And, now, did you plot the defendant's records?
A Yes, I did.
MR. SIMON: Can we look at Slides 23 and 24.
THE COURT: Let me just -- 26 meters is 26 yards; right?
THE WITNESS: Approximately. It's not exact.
THE COURT: That's two parking spaces?
THE WITNESS: Oh, I'm sorry. A few parking spaces. So a park space is typically about 3 meters wide. So that would be about, what did I say it was? Twenty-six. So about six to seven parking spaces.

THE COURT: All right.

THE WITNESS: And that's width, not depth?

THE COURT: Right.

BY MR. SIMON:

Q If we look at the -- particularly Slide 24. When you talk about a point extended beyond the geofence radius, which point, looking on Slide 24, is that point?

A The point that extends beyond is that point that's furthest north. And the center of that point is in the parking lot towards the north or the furthest north of the parking lot of the church.

Q Would it be fair to say that a very small portion of that display radius extends beyond the geofence?

A Correct, a majority -- a significant majority is withinside the geofence.

Q And every other plot point there is well within the geofence; correct?

A Yes, it is.

Q Now, did you also -- we've talked about Phase 1. What happens in the second stage of the warrant? How does that work?

A The second stage of the warrant is where Detective Hylton sent to Google a list of device IDs that were identified as being relevant to the investigation for

additional location data for those device IDs. And that would include, I believe, 30 minutes prior and 30 minutes following the original geofence time frame with no restraints on location, so that we can see the path of travel for these devices.

Q Is that the -- what we heard Sarah Rodriguez refer to as sort of the second stage, being that contextual Location History information?

A That's correct. It provides context for us so that if there is somebody that is just driving by, we try to eliminate them if we can. If there is somebody that is in another parking lot, still within the geofence and not in the area, we try to eliminate them, if we can, or we may need more additional information to evaluate them as a suspect and either eliminate or include them as a suspect.

Q Now, did you do the same thing that you did at the first stage with those second round records in terms of summarizing what we got back?

A Yes, I did.

Q All right. Looking at Slide 26, is this the -- are these the summaries of those records?

A These are. It summarizes the nine device IDs that we obtained records for from Google in Stage 2.

Q And it looks like the number of records this time

is a bit larger. We've got more records; right?
A That's correct. This time we received 680 records.
Q Okay. And if we look at the far right, there is a smallest maps display radius and a largest maps display radius. Describe those.
A That's correct. So, similar to how I analyzed the Stage 1 data, I also looked at the size of the display radiuses for the Stage 2 data. And those columns reflect the smallest display radius for that device and the largest display radius for each device.
Q And how many of those records in the second stage belong to the defendant's account?
A The defendant, again, device ID 1716665659, the second line from the bottom. We received 94 records for the defendant's device.
Q And this is a second stage that gives that additional 30 minutes on each side of the time, but also has no regard for -- at this point we're outside of the geofence now; right?
A That's correct. We can see the path of travel for each of these devices or if they were stationary for this time, we could see that as well. But it does not have the geographical constraints of being immediately in the area of the bank robbery.

Q And these second stage records, to the extent we get them, that's after a discussion generally between law enforcement, maybe the prosecutor and others involved; right?

A Correct. We evaluate each of the devices and determine if this device could be a witness to the crime, could be a suspect to the crime, could be an accomplice. We evaluate each of them to make a determination.

Q And what, if anything, goes into consideration of -- and particularly in this case, was there any consideration of the need to not only inculpate somebody, sort of inculpatory evidence, but exculpatory evidence?

A Absolutely. We would like to exclude as many people as possible. And we can use the second stage to do that, to make sure that we're looking at the person that's actually responsible for committing this crime.

Q Okay. In looking at Slides 27 and 28 -- I'm sorry, 28 and 29, are these the plotting of the defendant's records at Stage 2?

A Yes. So Slide 28 shows the complete records for the defendant in Stage 2 from about 3:50 p.m. through 5:50 p.m.

Q All right. Let's look at the left side here. Maybe we'll just bring it up by itself, Slide 28.

Can you walk us through the numbers here? Is this going in sequential order, the one through seven boxes here?

A Yes. So the first records we received are on the top of the page, the bubble to the right. The box is marked with a No. 1. There's two records in that area, both with the exact same latitude and longitude, the exact same center point. And those points are at 3:53:10 p.m. and 3:55:20 p.m.

The first point is 104 meters. And then we see that second point expand to nearly 1800 meters, which, again, is indicative to me of travel.

Then we see the device show up on -- towards the top left of the slide illustrated by Box 2 with a similar situation, 3:57:23 p.m. and 3:59:32 p.m., two records with the exact same center points, exact same latitude and longitude, the first one with a smaller display radius of 92 meters, and the second one with a larger display radius of over 1700 meters. Again, indicative of travel.

Q In looking at those two points, just to make sure we're talking about this right, this is prior to the robbery; right?

A Yes, it is.
Q And so these, again, are records at the second stage that are going to give us more context about where folks are moving?
A That's correct.
Q In looking at now -- you went through one and two. The third box here, can you go through those?
A Excuse me. Which boxes?
Q The third box of records on Slide 28.
A Yes. The third box contains the records in the immediate vicinity. Just about all the records for the geofence. And those are records for the time of 4:01 p.m. to 4:54 p.m. And those records are in that immediate vicinity of the Call Federal Credit Union and Journey Christian Church.
Q And so this is 54 of the records that we got at the second stage? I'm sorry. These are records that would be in both stages; right?
A Correct. Box 3 are records that would be -- not all -- I don't believe all of them are in the second stage, but most of them are. They're in that area.
Q Then you can -- can you walk us through what else we have here?
A Yes. Box No. 4 illustrates a GPS trail. So when I map these records, I think it's important to denote

the source of the record. So my red points are going to be GPS-based records and my blue points are going to be Wi-Fi-based records.

So we can see a trail in rapid succession more detail than we see anywhere else on this map of points from 4:58 p.m. to 5:04 p.m. with very small display radiuses of 3 meters to 10 meters leading away from the area of the bank robbery, down towards the area of 288, which is the road that traverses west to east on the bottom of the map.

Q Okay. Now, did you ultimately look at some sort of final records from this supplemental return?

A I did. Records 5, 6, and 7, those blocks, illustrate travel back towards the Mason Dale Drive area with the box with No. 7, the 18 Wi-Fi records, being in that immediate area of Mason Dale Drive.

Q In looking at Slide 29, is this the area of Mason Dale?

A Yes, it is. I've drawn all of the Wi-Fi points and the display radiuses on the map, as well as I tried to point out every residence that is either touched or in the area of those locations provided by Google.

Q What residence, ultimately, did Detective Hylton conclude, based on additional investigation, belonged

to the defendant?
A The address was 4702 Mason Dale Drive. The box is the second box down on the right side, which points pretty much to the center of the screen.
Q Now, using any of these particular Wi-Fi points, is it apparent exactly which house is hitting these Wi-Fi points?
A No. These records are not clear enough for me to say go get a search warrant to arrest or conduct a search of a house in this area. Additional investigative steps are needed in order to refine this data and determine where this device actually was located at this time.
Q Okay. And so this is -- this is the full extent of the second stage that we see here?
A That's correct, yes.
Q Okay. Now, looking at Slides 31 and 32, what happens at the third stage of the warrant?
A The third stage is where we go to Google again, and we submit to them the device IDs of which we want subscriber information for those device IDs. We requested three device IDs. And Google provided four things. They provided a file that maps the device ID that was in our geofence warrant to the account's Google ID. And based off that Google ID, they

provided the subscriber information for that account. And that's because that device ID is not a unique identifier across the entire Google-sphere. It is only a unique identifier within an account and within this geofence.

Q In looking at, on the right side, at Slide 32, is that the precise subscriber information we got for this defendant's device at the third stage?

A That's correct. So up top there's the table of the GAIA ID, which is the Google ID with the device ID that we mentioned before being associated with the defendant, 1716665659. We can see that that associated Google ID is listed in the subscriber information file that is on the lower part of the page, which is associated with the account that contains the name Jamaican Media with an email address of okellochatrie55@gmail.com.

Q Okay. Does it appear, the created on date there? There's a line that says "created on" on the right side on Slide 32. What is that?

A Yes. Three lines above the highlighted Google account ID there is a created on date, which indicates that this account was created on August 20, 2017 at 6:04 p.m. UTC.

Q And between August 2017 and July 2018, according

to Google records, Location History wasn't enabled on the relevant device; right?

A Can you repeat that question?

Q Well, let me ask it this way, because I think you have some facts about this. When the phone that the defendant enabled Location History on, the Samsung Galaxy S9, do you have a sense of when that phone came to market?

A I do. I believe --

Q It's Slide 38.

A Yes. It came to market on March 16, 2018, which is several months after the date of the creation date for this Google account.

Q Okay. And I think that my question that was going to be there, I'll just scratch that from the record. It wasn't to the point.

Now, with respect to the third round of information that we got on the three IDs, did you ultimately plot the points for the other two devices that we requested subscriber information on?

A Yes, I did.

Q Okay. Let's look at the device that ends in 2662 and Slides 33 and 34.

A Slide 33 indicates the one point that we received back, the one record of Location History that we

received in Stage 1 for device 907512662. And that plots a center point over the Journey Christian Church at about 4:35 p.m., prior to the time of the bank robbery.

Q Okay. And so why go back at the second stage here?

A Well, there are several reasons. So, the first reason is this is a device that was present in the area of the bank prior to the bank robbery. And we know that sometimes when people want to hide their location, they'll turn their phones off. And if their phone is turned off, no additional Location History would be reported for that device. So it's significant to us that there is a point inside the geofence that occurred prior to the bank robbery with no points after the bank robbery. Because we also believe that after a subject has robbed a bank, that they are going to flee the area and not be -- or not have any additional Location History records within this geofence several minutes after the bank robbery.

Q And, now, what about on the right side? Are we seeing the second stage records after we've requested the second stage on this device?

A That's correct. This is a plot of the second stage records which travel a bit in the area. The

first record that we have is 4:35 p.m. in the vicinity of the Journey Christian Church, and that's towards the top of the page with a call out box on the right side. That is the same point that we saw in the last slide.

The next reference point on the slide is travel towards the south ending up near box No. 2 where there are records at 4:47 and 4:53 p.m.

After this box, the phone retraces some of its steps north and then ends up near the apartment complex just south of the Call Federal Credit Union in Boxes 3 and 4. And to me, this is indicative of a trail of somebody that could have dropped off somebody in the parking lot, traveled a ways, and then returned to possibly pick up somebody that traveled through the woods between the Call Federal Credit Union and the apartment complex directly south of that area.

Q Okay. And there was a third device that we saw subscriber information on; correct?

A That's correct. That was device -1662304683.

Q And you plotted those points on Slides 35 and 36?

A Yes, I did.

Q All right. Now, tell us, when we pull those up on 35 and 36, what we see in Slide 35 at Stage 1 inside the geofence and why go back at Stage 2 and get

supplemental records on this particular record?

A Yes. These initial records that we received in Phase 1 shows us three Wi-Fi points. Two of the center points are directly on top of the Call Federal Credit Union and one location point is towards the right that covers the area of the Journey Christian Church. These points are between 4:44 and 4:47 p.m. And for the same reasons that I discussed prior, we know that subjects may turn off their phone to avoid transmitting Location History or device or being observed on the cellular network to obscure their location.

So with this device having points before and no points after, we thought this was -- we needed additional records to be able to see the context of this travel.

Q What about the second stage? Is that on the right side?

A Yes, Slide 36 provides that context of travel for us. And the first record we see is towards the center of the screen. There is a cluster of points marked by box No. 1 at 4:39 p.m.

There's another cluster of points that traveled northeast on Hull Street towards box No. 2, which is the area of the Call Federal Credit Union and the

Journey Christian Church. And those records are there at 4:44 through 4:47 p.m.

And then we see the phone travel back east -- I'm sorry -- travel west on Hull Street Road or appearing to be traveling -- appearing to be near Hull Street Road marked with box No. 3 at 4:55.

This becomes interesting to us because we see somebody that starts away from the bank, moves towards the bank, and then immediately leaves that area, which could indicate that they are dropping somebody off at that bank.

Q Now, just let me end with a question going back to Slides 23 and 24. We've talked about the investigation in this case and, in particular, I'm looking at the defendant's plot points on 23 and 24 when they come up. Did you and Detective Hylton reach a conclusion about whether this was the account, just based on Stage 1, that belonged to the person who robbed the Call Federal Credit Union on May 20, 2019?

A Based on several pieces of evidence, including witness testimony that indicated there was a suspicious blue Buick parked behind the church, which is notated on Slide 24 with the green box in the area where the red GPS points are clustered, combined with the video observations from the Journey Christian

Church and the Call Federal Credit Union, and the description of the individual and the visual of the individual, we determined that this was likely the device that belonged to -- that most resembled the device that would belong to the subject of the bank robbery.

Q And this is based merely off of the returns that came at the first stage that called for Google to only return devices that it determined were inside that geofence radius at the time of the crime; correct?

A That's correct. That is relying solely on that Stage 1 data without evaluating any of the contextual data that we received at Stage 2.

MR. SIMON: No further questions, Judge.

THE COURT: Cross?

MR. PRICE: Yes, Your Honor. Thank you.

CROSS-EXAMINATION

BY MR. PRICE:

Q Special Agent D'Errico, I just want to pick up right where you left off. You didn't stop at Stage 1 in this case; correct?

A No, we did not.

Q You still got the Stage 2 data?

A That's correct.

Q And you got the Stage 3 data, as well?

A That's correct.
Q Even though you were confident about your Stage 1 findings?
A We were confident in that was the device; however, the note that was passed to the bank robber -- or passed in the bank indicated that there may be additional suspects involved with this crime. So, in order to evaluate and investigate this crime fully, we felt that we needed to look at the other devices that could possibly be related to the investigation.
Q And, in fact, you ended up requesting account detail information on three of those devices; correct?
A I did not. Detective Hylton did.
Q Thank you. Have you received any specific training on geofence warrants?
A I have not received specific training. My training comes in the form of my education with my degree as a computer scientist, my education from James Madison University with a bachelor's in computer science, my training from Johns Hopkins University with my master's in security informatics. This training has provided me with the foundations to understand these complex topics of wireless communication and location data analysis. Pair that with my independent study of patents issued by Google

or obtained by Google and academic papers that discuss how it's possible to derive approximate locations using Wi-Fi access points and other reference material as well.

Q But you haven't received any specific trainings on geofence warrants?

A Google has not provided us any training on Google geofence warrants.

Q And there aren't any Justice Department policies on Geofence warrants, are there?

A I'm not aware of any policies, per se. We have policies that talk about investigative techniques that we can use, but nothing that focuses particularly on a geofence warrant.

Q And, similarly, there aren't any Justice Department procedures for obtaining geofence warrants, are there?

A There's not procedures, but in working with CCIPS, Computer Crimes and Intellectual Property Section of the Department of Justice, we are able to obtain what we call a "go by," which assists us in the language needed to obtain a geofence search warrant.

Q A go by. Could you explain a little bit more about that? Did you give one to somebody in this case?

A I don't recall that I provided any go bys in this case. But a go by, for us, is a document that has wording and points to remember to make sure we include in a search warrant. For example, Google has specific information that they need in order to process the search warrant. They need a location point. They need a radius or another shape to form that geofence. They also need a time period in order to obtain the records.

And then with the process that I understand has been discussed between CCIPS and Google, we follow the steps that they have laid out in order to work with or in order to serve Google with this search warrant to make sure that Google understands what we are requesting and that we understand what we'll receive back as part of that search warrant process.

MR. PRICE: Your Honor, we have long suspected that the government used a template of some sort in this case. We've asked for it repeatedly in discovery and have not received it. And so I would request that the government provide us with a copy of this go by so that we can review it.

MR. SIMON: Judge, we have -- we didn't use any Department of Justice go by in this case. I think it's been pretty clear that any request from

counsel -- and I'm not sure why this is coming up. We've had numerous conversations in this case. There have not been any discovery issues.

The questions were about whether Detective Hylton used go bys, what go bys he used. We told them as much as we could about that. He's going to testify. To the extent that they're asking for some Department of Justice go by, we've not declined to give them anything less than what we have.

And they certainly have Detective Hylton's federal search warrant. So I'm not sure what the go by discussion is. Every search warrant signed by any magistrate or any magistrate judge has some language that is "in consultation with others."

So I'm not sure what the point of this request is because we've given as much as we can give.

MR. PRICE: Your Honor, we believe that the go by is important to this case. We think that the sort of plug and play nature of some of these warrants raises serious questions about the potential good faith involved in the warrant process.

THE COURT: But wasn't the testimony that -- just that they didn't use a DOJ go by? Was access given to a DOJ go by in this case to anyone?

THE WITNESS: Your Honor, I didn't swear out

the warrant nor did I provide a go by to Detective Hylton in this investigation.

MR. SIMON: Judge, testimony would reveal, as defense counsel knows, that there was a federal search warrant obtained by Detective Hylton prior to this one, as well as, I think, another state search warrant or two. They have those search warrants that Detective Hylton obtained previously. Only one is under seal that they don't have. So I'm not -- I'm just not sure what we're getting at here, to be quite honest.

THE COURT: I don't see the relevance if it hasn't been used in this case and you have other information that pertain to Detective Hylton. If there's a sort of catch and replace process going on, he wasn't involved. He's using what you have the information about what he used.

MR. PRICE: It's also unclear to us where the language in Detective Hylton's warrant, even if it came from somebody else, originally came from.

THE COURT: I think that's just too far afield. There's no evidence about his turning to a DOJ go by. And any warrant is going to use language from previous warrants; from another agency, from another law enforcement program, from the state versus

the federal. That's the nature of how warrants are sworn out here. And if you have previous warrants he's used, I think that's what you're entitled to.

MR. PRICE: Okay. Thank you, Your Honor.

BY MR. PRICE:

Q You wouldn't say you know more about geofence warrants than Google; right?

A Google, the entity? No, I would not.

Q You don't have some unique knowledge that Google doesn't about geofence warrants; right?

A No, not that I know of.

Q So, for example, you don't know when and why Location History points are collected, do you?

A Yes, in particular, we do. We know that Location History points can be collected based on the testimony we heard earlier when a device is set up to opt in to Location History.

And if I could go back to the prior question, I don't know that Google is doing the analysis that we do on our search warrants when we see this information. And we learn a lot about this geofence data and this Location History data by reviewing and doing test observations and using this information in the field to ultimately recover a fugitive or a phone or somebody else that has committed a crime that's

been in that area.

So from the analytical perspective, using it in the law enforcement setting, I may have some more knowledge than Google because that is not how Google uses their data.

Q I'd like to show you an email that you sent to the government about this issue.

A Okay.

Q Page 15, please.

THE COURT: Of what?

MR. PRICE: I'm sorry. This is not in evidence, Your Honor. This is a set of emails that the government turned over in discovery in anticipation of Special Agent D'Errico's testimony.

THE COURT: All right.

So this is just to refresh his recollection?

MR. PRICE: Yes, Your Honor.

BY MR. PRICE:

Q Could you scroll down just a little bit.

So could you read the sentence that begins with "Few observations"?

A "Few observations. They really don't go into how they are determining location based on Wi-Fi, nor how they draw their display radiuses. I don't think we need to press them for it, but it would be nice to

know."

Q And then a little bit further down on the page. Could you read the highlighted line and the line right before it?

A "Here are some other things that would be good for Google to explain to fully understand this data. When and why points are collected. For example, in our case, there is a very frequent collection of Location History." And that sentence continues.

Q So you had confusion, at least at this point in time, about when and why Location History points were being collected?

THE COURT: We don't know when this was written, because you haven't put it on the record.

MR. PRICE: Sorry. This was written on March 9, 2020.

A I don't think there is confusion as to when Location History points are collected. I don't understand exactly at a certain time why a location point is collected, but I do understand that when the device is set up appropriately, that Location History will be collected.

Q Thank you. You understand how Google uses location data for advertising; correct?

A I do understand some ways that Google uses it, not

comprehensive.
Q And that this kind of advertising is, in fact, very lucrative for Google?
A I don't know of Google's exact breakdown on their location-based advertising.
Q You didn't prepare a slide on that for your CAST report?
A As far as location-based advertising, no, I did not. Advertising in general, yes. Advertising was about 86 percent of Google's revenue.
Q And you prepared other slides specifically about how they were using location data to conduct radius targeting and store conversion visits; correct?
A Sure. Is there a slide we can refer to?
Q Yes, there is.
MR. SIMON: Judge, I'm not obviously going to object. It's in the presentation. I would just note that I didn't ask any direct third-party doctrine-related questions.
THE COURT: I'm just going to let the record be full. And the whole slide is in.
MR. SIMON: I understand, Judge.
BY MR. PRICE:
Q Can I draw your attention to Slide 40, and Slide 50, and Slide 40, 41 and 42?

THE COURT: 40, 41 and what?

MR. PRICE: 42, Your Honor.

Q On Slide 40, you're demonstrating that Google is a profitable company; correct?

A I'm demonstrating the revenues, and particularly the point of this slide is to discuss the amount of advertising revenues that comprises Google's entire revenue as well as the main products that Google uses. That was per their 10K reports and other information.

Q Thank you. And the main Google product that drives its revenue is what?

A I believe it's advertising.

Q Thank you. Can we go to the next slide?

Here you have a slide on target ads to geographic location, and you refer to something called radius targeting; is that correct?

A That's correct. On Slide 41, it illustrates some of the information on the Google ads help page, which indicates that a company can draw a radius around a location in order to target ads.

Q Thank you. Can we go to the next one. And here's a slide about store visit conversions.

THE COURT: Slide about what? You really are --

MR. PRICE: Store visit conversions. Sorry,

Your Honor.

THE COURT: Okay.

A Yes, Slide 42 does talk about store visit conversions similar to what Mr. McGriff talked about earlier today.

Q Thank you. And this is a method of advertising for Google based off of location?

A This is information that Google had on their website, on their Google ads site.

Q And it's about advertising using location data; correct?

A I believe these are metrics that they can provide back to folks that place ads.

Q Thank you. Okay.

So advertising based on location data is not the same thing as serving a geofence warrant on Google; correct?

A Can you repeat that question, please?

Q Advertising based on location data in not the same as serving a geofence warrant on Google?

A I don't know that I can draw that conclusion.

Q Well, when businesses place ads with Google, they don't receive any location data about the users and devices they're trying to target; correct?

A That's correct.

Q And they can't ask for more data on where people saw their ads, can they?
A I don't know what they can ask for.
Q They can't ask for more information about where someone went 30 minutes after seeing an ad; correct?
A I don't know that information.
Q It's true for store visit conversions that Google does not provide user location data directly to those businesses?
A I believe Mr. McGriff testified today that they don't provide location data to folks that -- companies that do ads. I believe his testimony was that they provide information in aggregate that no longer resembles an individual's location.
Q Correct. And the same is true for radius targeting, as well; right?
A The same -- can you repeat that?
Q Businesses who engage in radius targeting do not get user location data as a result from Google?
A I'm only aware of Mr. McGriff's testimony today.
Q So the only reason the government was able to obtain Location History data in this case from Google was because they served them with a warrant; right?
A There -- well, there are a couple of factors. There was Location History turned on, and there was

Location History available. And the government served a search warrant for those records which were held in Sensorvault because the Location History was enabled on the defendant's phone, which allowed Google to be responsive to the search warrant that was obtained and served by the government.

Q So Google wouldn't have compiled these records and sent them to you if you didn't serve them with a warrant; correct?

A They serve them in exigent circumstances. They are responsive to law enforcement if we request, using a search warrant or other legal process, for records that they hold.

Q Have you ever obtained geofence data without using a warrant?

A I take that statement back. Google is very particular about that and does not allow it on exigent. They will allow Location History on exigent circumstances but still insist that we obtain a search warrant on a geofence. Thank you for allowing me to correct that.

Q Thank you. And the warrant here required Google to do things with location data that it would not do for any business seeking to advertise through Google; correct?

A I'm not aware of all of Google's business practices.

Q Would Google conduct a geofence search for an advertiser?

A Again, I'm not aware of Google's practices.

MR. SIMON: Judge, I think we -- I'm trying to be fair about this and not stand up unnecessarily. We've had two Google witnesses discussing this search warrant. They've been asked questions. They've answered them. The expert's been in the courtroom. Why we're going down the path of asking FBI Special Agent D'Errico about Google's internal business practices, which everybody is going to agree Google is the best evidence of that, I don't understand the relevance and why we continue to go down this path with this witness.

THE COURT: Sustained.

MR. PRICE: I'll move on.

BY MR. PRICE:

Q So you compare the area of the geofence warrant in this case to the area of a hypothetical tower dump; correct?

A Are you referring to a particular slide?

Q Yes. In your presentation, the one with the -- let me pull it up for you. This would be Slide

No. 21.
A Could you repeat your question?
Q So, in your report, you compare the area of the geofence warrant in this case to the area of a hypothetical tower dump?
A Yes. We didn't actually obtain this tower dump, but based on my training and experience with cell phone towers, this is the best representation that I could draw of the approximate coverage area of that tower dump.
Q Would you agree with Google's statement in its amicus brief in this case that a tower dump requires a provider to produce only records of the mobile devices that connected to a particular cell tower at a particular time?
A Yes.
Q So you suppose the area of the tower dump in your hypothetical based on three Sprint towers nearby the bank; correct?
A That's correct. This is an example of a tower dump for Sprint. We would also do a tower dump for T-Mobile, Verizon, and AT&T, or any other carrier that provided service to this area. And that drawing would look different because they have towers in different places.

I chose Sprint in this case because Sprint is the service provider for the defendant's phone.

Q So in your hypothetical, you suppose the area of this tower dump based on three Sprint towers? That's it.

A No, that's not it, actually. I drew this line using many of the towers that are on this page, because what we know about cell phone towers is that they -- and this is information that we have learned directly from the carriers because our training includes training by network engineers at the telephone companies, including Sprint, that when they're planning out their network, they place towers where they need coverage areas, and they do not place towers where they do not need coverage area. And their goal is to provide a certain level of customer satisfaction, and that includes providing coverage area. And that coverage area, it can be determined by approximating maybe about 70 percent to the next tower.

So in my drawing, in my estimation of the area of the tower dump, I looked at each of the three towers inside that I selected, and then I drew my line approximately 70 percent to its nearest tower. And that's how I approximated the area of the tower dump.

Q So you looked at a map to see where the towers were?
A Yes, I plotted the Sprint towers.
Q And then you drew a line around that area to indicate the coverage of those towers?
A I drew the line to indicate the approximate coverage of the areas. We don't know the exact coverage of the areas, but based on a map and based on my training and experience, this is an approximation of the area that would be covered in a tower dump if we were to do one for that area.
Q Thank you. And you can see on the satellite map whether the area is an urban or rural area?
A I can tell if there are greenery or major roads or even some secondary roads. I don't have a complete listing of what is in each of these locations.
Q Okay. By looking at a map like this, you could begin to approximate how many people might be affected by the hypothetical tower dump here; right?
A It depends on many factors. It depends on businesses. It depends on travel. That's not something that I estimate.
Q But because of your training and experience as a CAST team member, you would know that each tower has a maximum number of users that it can handle at one

time?
A That's true. There is a maximum at one time.
Q That's called a tower load?
A I don't have an exact phrase for it, but there is an upper number of which there will be a point where the tower will be saturated and no additional phones would be able to make any communications off of that tower.
Q Overloaded towers, they'll drop calls if there are too many people trying to connect at the same time or transfer them to another tower?
A It depends. So cellular communication is complex, and there's lots of different factors at play. So just because -- let me particularize this to Sprint. If we were to ask Sprint for a tower dump, Sprint would be able to provide calls that were originated and ended in this area during the time frame that we requested.
Q So in a hypothetical like this, of course dealing with Sprint -- by the way, when you get tower dump results from Sprint, those are only for people who use the network for either phone calls or text messages; correct?
A I believe I just answered that.
Q It doesn't include data transfers?

A Sprint at the time of this would not have included data.

Q So if you did a tower dump on just one of these Sprint towers, you would have a rough idea of the maximum number of users you could possibly get in an hour period?

A I don't have a maximum number. I'm not aware of what the maximum number is.

Q Mr. McInvaille testified yesterday that according to your hypothetical, you'd probably net about a thousand users per tower. Does that sound about right to you?

A I don't have a frame of reference for that. I would not be able to make an estimate on that.

Q Do you have any information that would contradict Mr. McInvaille's estimation?

A I'm trying to recall back to tower dumps that I've seen before. I just -- at this point I don't have a good frame of reference.

Q So you don't have anything to contradict Mr. McInvaille's conclusion?

A I don't. Not at this time.

Q Thank you.

So you're aware that Location History information is determined differently than cell-site location

information; correct?
A As it's -- can you rephrase that question?
Q You're aware that Google Location History information is calculated differently than cell-site location information?
A It can be, but it's not always. It depends on how the cell carriers are determining locations for phones. So a cell carrier could use the GPS sensor in a phone to determine a location of the phone.
Q Could a cell carrier use the Wi-Fi networks, the Wi-Fi fingerprinting that you described earlier in your testimony?
A I don't think so. I don't think that's part of the E911 Phase 2.
Q So it's calculated differently than just plain old CSLI; right?
A Not all information is calculated differently.
THE COURT REPORTER: CSL?
MR. PRICE: CSLI, cell-site location information. I apologize.
BY MR. PRICE:
Q Location History data is usually calculated using GPS or Wi-Fi; correct?
A We see sources of GPS, Wi-Fi, or cell fairly regularly.

Q There are no cell records in this case; correct?
A That's correct, no cell records in this case.
Q And Google prefers to use Wi-Fi or GPS before using cell data; correct?
A I don't know what their preferences are.
Q Did you listen to Mr. McGriff's testimony yesterday?
A I did listen to it.
Q And he explained that cell-site location is less preferred because it's less accurate, generally speaking?
A I don't remember his exact testimony about that point.
Q Okay. In any case, with GPS and Wi-Fi fingerprinting, there are no cell phone towers involved; correct?
A That's correct.
Q Okay. So that means there's no way to get Location History data just by identifying nearby cell phone towers?
A In this case, there were no Location History records obtained using exclusively or primarily the cell phone tower. I don't know that the cell phone tower was not included in the calculation for Wi-Fi or GPS, but I know there were no records marked cell,

which to me would indicate that the cell tower would be the primary sensor used to determine Location History.

Q So you have to rely on Google to determine which devices were present. There's no way to identify a couple of towers nearby; correct?

A There is a way to identify a couple of towers nearby, and we could have obtained a tower dump to obtain that information. In this case, we did not.

Q Let me rephrase. I mean that Google will not respond to a request for Location History information based on the location of a cellular tower; right? They testified earlier today that they do not index their Location History database in that manner.

A I'm sorry. I'm not understanding the question.

Q Google testified earlier today that they do not index their Location History database by location. They index it by user.

A Is that a question?

Q Was that your recollection of Google's testimony, as well?

THE COURT: How did they hold stuff in the Sensorvault. That's the testimony he's talking about.

THE WITNESS: Yes, I understand that -- I believe it was Ms. Rodriguez that said that they have

their Sensorvault data indexed by user, whether it was device ID or Google account. I believe it was indexed by Google account.

BY MR. PRICE:

Q We can turn to Google's amicus, as well. Google explains -- I believe this is page 14 of Google's amicus brief, Defense Exhibit 2. Google says, "The steps necessary to respond to a geofence request are thus quite different from and far more intrusive than responses to requests for a CSLI or tower dumps"?

A Which page is that on?

Q This is page 14 of the amicus brief. It's the highlighted language or will be highlighted in a moment.

A I see that paragraph, yes.

Q You don't disagree with that, do you?

A That it is more intrusive? I don't believe that it is more intrusive.

Q They go on to explain, they say, A tower dump requires a provider to produce only records of the mobile devices that connected to a particular cell tower at a particular time. But because Location History is different, Google has no way to identify which of its users were present in the area of interest without searching the Location History

information stored by every Google user.
A I see that paragraph, yes.
Q You disagree with that?
A So, I don't -- it's hard for me to compare because I don't know exactly how the cell phone carriers store their data. If their data is stored in a central database, then they have to search every record in their database to obtain the tower dump records. So I don't know that I have enough information to fully evaluate that.
Q So you don't have enough information to contradict their statement that says Google has to search across all Location History journal entries -- I'm sorry. We're on page 12 to 13, the bottom page 12 to the top of page 13. Instead, Google has to search across all Location History journal entries to identify users with potentially responsive data --
THE COURT: Don't read it too fast.
BY MR. PRICE:
Q -- in order to comply with the request.
A Do I disagree with that? No. They need to do a search of the Sensorvault database for locations that are responsive to the geofence.
Q And you don't have any information to contradict their next statement that Google has to run a

computation against every set of coordinates to determine which Location History records match the time and space parameters of the warrant?

A I don't have any information to contradict that.

Q Do you know how many users had Location History enabled when Google executed the geofence warrant here?

A I only know the information that was provided by Mr. McGriff and his affidavits, which I believe he talked about tens of millions.

Q That's right. Google says that roughly one-third of active Google users had Location History enabled on their accounts, and that that translates to numerous tens of millions of Google users. You don't disagree with Google about that, do you?

MR. SIMON: Judge, I'm going to object again to, I think, questions that are basically attempts to testify. Asking this witness who says he has no personal knowledge of Google's internal practices, the Court has already sustained that objection. I think we should move off, Judge, based on relevance this and also personal knowledge, asking questions about Google's internal process.

This witness is going to consistently say Google's got the best answers on their internal

process.

MR. PRICE: We can move on, Your Honor.

THE COURT: Okay. Good.

BY MR. PRICE:

Q Regardless of the ultimate number, they're searching everybody with Location History enabled at the time; correct?

A Again, I have to defer to Google on that. They conduct the query of their database.

THE COURT: That's actually not moving on.

MR. PRICE: Okay. We can move on to the next part.

BY MR. PRICE:

Q Records from a Sprint tower dump don't show every device that's in the area; correct?

A No. Records from a Sprint tower dump show the devices that were making calls or receiving calls in that area that were on the Sprint network.

Q So, in addition to being on the Sprint network, as we just discussed a second ago, a user would have to be making a phone call, receiving a phone call, sending or receiving a text message to show up in that tower dump with Sprint?

A Yes, with Sprint. There has to be a network transaction occurring.

Q I want to get your take on whether you agree with Google here. They say, on page 9, of their amicus brief --

THE COURT: Wait a minute. Didn't we just have an objection to this, that this witness can't say whether or not this is the best answer that Google does? So you can go through the whole brief. He's already said to you he can't agree or disagree because Google knows the answer, and he doesn't. Am I wrong about that? Well, it doesn't matter, because I'm saying you can't ask it.

MR. PRICE: Yes, Your Honor.

BY MR. PRICE:

Q In fact, law enforcement did not get a tower dump in this case; correct?

A That's correct, we did not get a tower dump.

Q And it wouldn't have been useful, at least for Sprint, if the suspect did not make a phone call, receive a phone call, send or receive a text message during this time?

A If he did not, but he did.

Q A tower dump would not have registered him if he did not?

A That's correct. If he did not make a call, the tower dump would not register that. If he did not

make a call or a text or receive a call or a text.

Q And even if the suspect did show up in a tower dump in this case, you wouldn't have any way of identifying that suspect based solely on the tower dump in one instance?

A That's incorrect. So our investigative plan would have been to compare the tower dump to a list of blue Buicks, owners of blue Buicks, that we were prepared to obtain from the Department of Motor Vehicles. Whereas, one tower dump alone sometimes is not enough, we did have another data set to compare it to even if it was not a tower dump.

So in that case, this case, we were prepared to obtain data from the Department of Motor Vehicles of blue Buicks, the same vehicle that was reported to us by a witness being behind the Journey Christian Church, the suspicious vehicle, and compare the registered owners of those vehicles to the phone numbers in the tower dump.

Q So you're saying there was another way you could have worked this case without doing a geofence warrant?

A What I'm saying is there's many investigative techniques out there, and the investigative technique that we used first was the Google -- or that we used

prior to using the tower dump was the Google geofence.
Q So there was another way you could have done this, but you chose not to?
A I didn't make that decision.
Q The government chose not to?
A I think I answered that question. The first technique that we decided to use or the technique we decided to use earlier was a Google geofence. And if that had not had results, that we did have other investigative techniques that we could have used.
Q Thank you. You said you used 2703(d) orders to obtain tower dumps. Is that still true?
A Yes, it is.
Q You don't get warrants for those?
A No, we do not.
Q Not even after the Supreme Court's decision in *Carpenter*, 2018, requiring a warrant for cell phone location -- historical cell phone location information?
A No, it is not required. *Carpenter* does not comment on tower dumps, nor does it comment on location data less than seven days.
Q So it's your practice not to get warrants for tower dumps?
A There is discretion that a 2703(d) can be used for

a tower dump or a search warrant can be used.
Q You said you don't tell companies how to conduct a search in the case of a tower dump, for example?
A I am not an expert in their internal systems. We provide a search warrant with the information that we are requesting on their records. They conduct the -- they obtain those records, however they will, and they provide those to us.
Q So you've never seen a search warrant for a tower dump that specifies the towers to be searched?
A Sometimes we do specify the towers to be dumped because we have information that those towers would cover the area in question.
Q That is in your hypothetical, for example, with Sprint?
A Those are the towers that I likely would have searched or requested be searched for a tower dump.
Q Okay. So when Google produces data in response to a geofence warrant, they include this display radius; correct?
A That's correct.
Q And in his first declaration, Mr. McGriff wrote that a radius -- let me just pull that up. It's Defense Exhibit 21, Mr. McGriff's first declaration at page 9. And Mr. McGriff wrote, "A radius around a

user's estimated location that shows the range of location points around the stored Location History coordinates that are believed to contain, with 68 percent probability, the user's actual location."

A I see that in paragraph 25.

Q And you understand that 68 percent to be Google's confidence that somebody is within that display radius?

A I believe that is exactly what it says. That if they see those conditions 100 times, 68 percent of the time that it will be inside that geofence or, excuse me, inside that map display radius.

Q And 68 percent is the industry standard for this; right?

A 68 percent is approximately the industry standard, yes.

Q But regardless of that 68 percent confidence, if a user's estimated location falls within the radius of the geofence, then Google treats that user as falling within the scope of the geofence; correct?

A If the center point of the Location History record is within the geofence, then Google does provide it responsive to a search warrant.

Q Even though there's no greater probability that the user is in the dead center of that display radius

as opposed to off by the edge?
A That's correct. Google doesn't provide a percentage that it's going to be in the northwest corner versus the northeast corner versus the south of that map display radius.
Q And the map display radius often extends the geofence as drawn?
A I don't agree with that characterization. I don't think it often extends beyond on our Stage 1 data.
Q It does -- it extends beyond the geofence in this case; correct?
A There are select points that extend beyond but not -- nowhere near a majority of points.
Q Okay. But that fact, the fact that the display radius exceeds the geofence circle, means that false positives are possible when you conduct a geofence warrant; correct?
A It is -- I believe Google testified to it. They are making a good faith effort to determine the location of that device. Their technology is not 100 percent, but they are providing a good faith effort in order to determine the location of that device.
Q So you agree with Google, false positives are possible?

A False positives are possible.
Q Was there a false positive in this case?
A I don't know.
Q Perhaps one of the three that made it all the way to Stage 3?
A Could you -- which one would you like to discuss?
Q Let's take a look at your report on page 31. The user with device ID 2, ending in 2662?
A 907512662?
Q Correct. That was one of the three device IDs that made it all the way to Stage 3; correct?
A That's correct.
Q Can we look at page 34 of your report. This is the Stage 2 data plotted for that device ID; correct?
A That is correct.
Q And there's only one point in all of that data that falls within the geofence as drawn; correct?
A There is one center point that is in the geofence. There is another GPS point that has its display radius overlapping into the geofence.
Q And when you were looking at this data, did you consider the time intervals between data points?
A Yes, I did.
Q And were you able to determine from that time, from those intervals, whether this individual was

likely walking or driving?
A I don't remember my exact assessment. Looking at this data now, it appears that the person was traveling at vehicle speeds.
MR. PRICE: And can we please bring up Defense Exhibit 5.
BY MR. PRICE:
Q This is the three-paths video that Mr. McInvaille created detailing the Stage 2 data for three of the individuals caught up in this geofence. This is the user that we have referred to as Mr. Blue. I'd like to play the video for you so you can see the trail of his data as it goes and touches inside of that geofence.
(Video is played.)
Q So based on the time lapse in between those points and the fact that they are almost all on roads, you were able to determine that that person was likely driving?
A Well, in that case, I can't eliminate that the person ducked into that parking lot, dropped somebody off, and then continued north on Price Club Boulevard.
Q Can we take a look at Price Club Boulevard there and ZOOM back for a second.
So, somebody driving along Price Club Boulevard

from the south of our screen up to the north would have to drive on the road; correct?

A Yes.

Q They couldn't drive through the trees and right over the church and onto the road on the other side; right?

A That's correct. If you're driving in a vehicle, generally you need to stay on the roads.

Q So, based on your training and expertise, looking at this data, isn't it likely that this person was driving on the road next to the geofence?

A Again -- well, it appears that they approach, but I cannot rule out that that person did not turn into the parking lot, drop somebody off, and then resume travel on that road.

Q So if false positives are possible, false negatives are possible, too; correct?

A Yes, they are.

Q Okay. So you testified that the effective geofence radius here, that was your words, "effective geofence radius," was 150 meters?

A That's the radius that we requested from Google, and they were responsive. All points fell withinside. All of the center points for the Location History data fell within that geofence.

Q So that's the requested geofence radius; correct?
A Yes, that's the geofence radius.
Q The effective geofence radius would have to take into account the display radius for all the different location points; correct?
A It is possible that that device is outside the geofence. It is also possible that point is inside the geofence. I don't have enough information to evaluate that.
Q The display radius means that the geofence, when it is run, as we just discussed, may pull in people as a false positive who were not, in fact, inside that geofence; correct?
A Yes, it's possible.
Q So they would be, then, outside the geofence and mistakenly labeled as inside; correct?
A Yes, that's possible.
Q So if it is pulling in people who are outside of the geofence as drawn, the effective range of that geofence must be larger than the geofence as drawn?
A The person could be outside the geofence. We just don't have enough information to evaluate exactly where they are.
MR. PRICE: Could we look at Slide 22, please. Slide 20, my apologies.

BY MR. PRICE:

Q So, in this case, the one user who had a display radius of 387 meters based on Google's data, there was a 68 percent chance that that person was somewhere inside that very large blue circle; correct?

A That's correct based on Google's testimony. There is a 68 percent chance that they're inside that circle.

Q So the effective range of this particular geofence warrant exceeded the geofence as drawn by, what was it, 290 meters?

A I can't agree with that conclusion because we don't know the actual location of the device. That bubble covers the entire geofence, and that device could be inside the geofence. It could be outside but it could also be inside. So I can't really evaluate that because I don't have enough information to determine if that device was actually inside or actually outside. And that's the thing about this data. They are estimated locations for us, so that we can determine the estimated location of the device in order to move forward our investigation.

Q As you testified earlier, it's just as likely that someone is at the center of that big blue circle as it is that they are right by the edge; correct?

A Google doesn't provide any indication where in that display radius they are. They just provide the display radius, the center point, and say it's a 68 percent chance that they are in that area.

Q So there's a 68 percent chance that, say, the user was standing at the edge of that circle 290 meters outside the geofence?

A No, I think your math is incorrect. What Google is saying is there is a 68 percent chance that they are inside that geofence. They're not saying that there's a 68 percent chance that they are at the intersection of Hull Street and Price Club Boulevard, and they're not saying there's a 68 percent chance that they're down in the cul-de-sac at the bottom. They're saying there's a 68 percent chance that the device is inside that geofence.

And that is, yep -- and that's what they have provided to us.

Q That's fine. Thank you. You don't know exactly why the display radius was so big for this particular user, do you?

A I don't know the exact reasons, but based on my knowledge and analysis of previous Google location records, this indicates that there was some travel, some motion on this device, because the point prior to

this large radius was the exact same latitude and longitude as this large point, and the first point was also a much smaller radius.

Q So there could be any number of reasons why that one point generated such a large display radius here?

A I'm aware of that reason for it, but there may be others, yes.

Q And you don't know exactly how Google calculates their display radius; correct?

A No, I don't. That's a Google question.

Q That's sort of their secret sauce, isn't it? It's proprietary is what I mean to say.

A I don't know. They have not provided it to us.

Q When you use Google's API to estimate your display radius for the drive test that you do, you don't get to see the calculations that Google does. You just send it off to them; correct?

A That's correct. I just send the information to Google, and they respond back with a latitude and longitude and a display radius.

Q That's because their algorithm, their way of calculating that display radius is considered proprietary?

A I don't know if they've marked it proprietary. I'm not familiar with their internals.

Q But you do know that the display radius can be quite large. In fact, much larger than 387 meters.
A I have seen large display radiuses before, yes.
Q And the largest one in this case was 1,842 meters; correct?
A I don't know off the top of my head, but I see a large one in Stage 2 data of 1,842.
Q Any others?
A Sure. There's another one that's 1,797 meters.
Q And there is one that is 1,838 meters, too; correct?
A Yes. Those three points out of the 680 are large.
Q In fact, there were three others with display radii exceeding 1,000 meters here. There are four points.
A In see four points listed on Slide 26. That's what I'm referring to when I look at the large map display radius.
Q Okay. Thank you. So, to sum up, you don't know how big the display radius is going to be for any given point before you do the geofence warrant; correct?
A That's correct.
Q You don't know how the display radius is actually calculated?

A That's correct.
Q You don't know how far beyond the geofence it's going to extend?
A That's correct.
Q And you don't know how many hits you're going to get in Stage 1?
A That's correct. That's why we ask Google for the information with the search warrant.
Q You haven't seen Google's policies on responding to geofence warrants?
A I'm assuming those are internal policies. I have not seen any.
Q So you don't know how big a radius is acceptable to Google?
A These are -- I'm not aware of Google's internals.
Q And if you get Stage 1 data, you're not certain how many users Google is going to provide Stage 2 data for; correct?
A Google provides Stage 2 data for the users that we request following the narrowing process.
Q There's no fixed number of users that you have to narrow it down by between Stages 1 and 2; right?
A Not that I know of.
Q So, it's sort of up to -- it's a bit of a negotiation with Google about what is acceptable in

terms of Stage 2 returns?
A Well, it's written pretty particularly in the search warrant that the government -- I believe it's will attempt to narrow. And that is that's part of the process.
Q And if they attempt and Google doesn't find it sufficient, what happens?
A Google will come back to us initially, and they may say -- or they may want to have a discussion on what the circumstances are. I was not part of that in this case. I can't speak to what happened in this case as far as that.
Q And the same sort of discussion process would happen between Stages 2 and Stages 3; correct?
A I know that based on the testimony of Ms. Rodriguez today.
Q And the geofence warrants that you've dealt with?
A Generally, when we ask for the device IDs, we have narrowed it down sufficiently and Google provides those.
Q So you've had these discussions with Google before?
A No, because we have -- Google has been responsive to the geofence warrants that I've submitted.
Q Okay. Thank you very much.

A Yes.

MR. PRICE: No further questions, Your Honor.

THE COURT: All right. Is there any redirect?

MR. SIMON: Judge, I'd ask three questions and --

THE COURT: Okay. And then we'll take a recess.

REDIRECT EXAMINATION

BY MR. SIMON:

Q Can we pull up Government's Exhibit 1, Slide 24.

Special Agent D'Errico, you were asked about a lot of plot points, none of which -- the large display radius had nothing to do with the defendant's account; correct?

A That's correct.

Q And if we're talking --

THE COURT: Okay. I don't know why. I'm really having trouble. Move the microphone up so it sort of captures you.

MR. SIMON: I didn't fix the mic, Judge. You're right.

BY MR. SIMON:

Q Special Agent D'Errico, the discussion about the display radius for that one point that was considered

relatively large, that was a different user's account, not the defendant's account; correct?

A That's correct.

Q And if we're talking about the defendant's account, we would be looking at Slide 24; right?

A That's correct. Slide 24 shows the initial Stage 1 data for the defendant's phone.

Q And so if we're talking about that 68 percent, I want to be clear about it, the 68 percent number relates to the fact that the individual to Google's best estimate based on its technology would be within that blue display radius; right?

A That's correct, that blue display radius. And you can see some of these points in yellow are right on the edge of those display radiuses. So they can be anywhere in there, but these points are consistent with the defendant being in those locations.

Q Okay. And with respect to the search warrant and what the search warrant requests from Google, it asks Google to send us back who you have determined is within the red geofence radius; right?

A That's correct.

Q Now, the accuracy of Google points, you've done some testing we talked about; right?

A Yes, I have.

Q What have you determined about the accuracy of Google's location points if you've come to a percentage yourself in terms of your own location points?

A I don't have a particular percentage, but what I've learned is that sometimes Google is a little too conservative with their display radius, particularly in Wi-Fi points, and that sometimes Google misses the mark by several meters. Single digit meters. So the point would fall outside of the display radius, but it is still in the immediate vicinity of the area.

So, for example, if a point -- from this data, what we're seeing is that the device is in this area. This is not saying -- it's not a miss such that the device is in California or Illinois or even north of Richmond. When we have seen misses by the Google location data, it's by very small amounts, especially in areas like this that have Wi-Fi coverage. And that actual location might be just outside of the map display radius that they show.

So, whereas Google does aim for 68 percent inside, there is a percentage that is right outside, just outside that display radius based on the observations that I've had.

Q When you say "conservative," can you just explain

what you mean by that word "conservative"?
A Yes. That Google has made -- I'm sorry. Maybe that's not the right word. Google has made that display radius a little smaller than it should have been. And that if Google increased its map display radius by 10, 20 meters, that point would fall inside that new display radius. So what I'm saying is when a point misses, it's outside the 68 percent, it's generally still in that area. It's a near miss, not a flagrant miss of putting a device in Washington, D.C., or even the other side of Chesterfield County.
Q Okay. And then, last question, looking at Slide 28, the supplemental records for the defendant's phone, there was some talk about the large display radiuses at the second stage when we've moved outside of the geofence and asked for records -- for these additional records for these devices.
Looking at, again, box 1, that's one of those large points, 1797 meters. Two minutes before, it's 104. Again, what is that indicative of based on your training and experience?
A That's indicative of travel. So in boxes 1, the two points have the exact same latitude and longitude. So there's a single marker in the middle. And what happens is that first point is a hundred-meter radius,

104-meter radius. And for some reason when the phone goes to take the next measurement, which is about two minutes later at 3:55, for some reason unknown to me the center point is not updated to a new latitude and longitude.

But what happens, I believe, is based on the sensors in the phone, the accelerometer, which determines speed, and the gyroscope, which determines tilt, is that using those additional signals, it can estimate approximately how far away that device is.

So we still deem these accurate even though they are a larger circle. It may not be as precise, but it's still accurate as to the device is somewhere in that area.

MR. SIMON: No further questions, Judge.

THE COURT: So, I'm going to ask one question I really don't want to open up a can of worms, but I just want to be clear. If Google is saying in the display radius, there's a 68 percent chance that the device is in that radius, what does the other 32 percent reflect? That it's not there?

THE WITNESS: That the device would be outside of that display radius. And in my experience with testing this data and doing my own measurements, a lot of those points are what I would characterize as

near misses, which means still in the general area, but maybe they're a football field away. Maybe they're 100 meters away. Maybe they are 20 meters away. But they are still in that general area. And we are not looking at folks that are in Washington, D.C. or other geographic areas. That's been my experience with this data.

THE COURT: All right.

MR. SIMON: Nothing further, Judge.

THE COURT: Can this witness be excused?

MR. SIMON: From the United States, Judge, yes.

MR. PRICE: For the defense, yes, Your Honor.

THE COURT: All right. Thank you, Special Agent, for your time.

THE WITNESS: Thank you.

(The witness was excused from the witness stand.)

THE COURT: We're going to take a recess. I'd like to keep it just to 6:15. That's only 12 minutes, but I am being the antithesis of an Eastern District judge. I have had trials here where somebody told me at lunch to cut my witness list in half because I was taking too long. So I really just want you all to get your job done, but also be mindful of

everybody's time, especially with asking repetitive questions. All right. Okay.

(Recess taken from 6:03 p.m. to 6:15 p.m.)

MR. SIMON: DO we need to put him under oath, Judge?

THE COURT: Yes, of course.

I was going to say we're going to put him under oath. Detective Hylton, we'll ask you to stand for that.

I'm also going to say that it's been a long day, and we cannot go any more than an hour without a break. So if you guys understand that, there are a lot of people here who are very tired. And so I'm going to accommodate them, of course, as I have you perhaps a little too much. So one hour per break. And it really would be nice if we ended in an hour.

All right.

JOSHUA HYLTON, called by the United States, first being duly sworn, testified as follows:

DIRECT EXAMINATION

BY MR. SIMON:

Q Detective Hylton, can you state your name for the record, please.

A Yes, sir. It's Joshua Hylton, spelled H-Y-L-T-O-N.
Q Okay. And you're a Task Force Officer with the FBI; right?
A That's correct.
Q And which task force are you with?
A The Violent Crimes Task Force in Richmond, Virginia.
Q How long have you been there?
A Since December of 2016, sir.
Q And you've been in law enforcement since 2011; right?
A That's correct.
Q With Chesterfield?
A Yes.
Q Police Department?
A Yes, sir.
Q Okay. Now, when you started your career, what kind of crimes did you investigate?
A Initially, as a patrol officer, just the average patrol-type crimes, larcenies, things of that nature, assaults, vehicle infractions. And, I believe, in August 2015 I was assigned to our Persons Unit who investigates violent crimes to people.
THE COURT: Did you say "Persons Unit"?

THE WITNESS: Yes, ma'am, in Chesterfield.

So that's what we called it at the time. Now we've broken it up into sections of robbery and homicide.

When I was first assigned to the unit, I investigated homicides or suspicious deaths, missing persons cases, natural deaths, accidental deaths, robberies to the person, whether it be a street robbery or what we call a drug rip robbery, or, of course, a commercial robbery, as well.

THE COURT: Drug rip?

THE WITNESS: Yes, ma'am. Essentially, a drug deal that has gone bad for one party or the other where someone will attempt to purchase whatever drug it might be, and then they get robbed. I apologize for the term.

Commercial robberies, such as bank robberies, major assaults, shootings, rapes, things of that nature.

Q How many robberies have you investigated?

A It's hard to say, as a primary investigator, but at least well over 100.

Q Okay. Did any of those robberies involve alleged conspiracies?

A Yes, sir.

Q Have you gotten any training in your role as a law enforcement officer?

A Yes, sir.

Q What's that?

A Well, the Chesterfield County Basic Police Academy, which lasted over seven and a half months, approximately two months of field training with another officer or more experienced officers. Likewise, when I became a detective, we had a period of training where we had to be evaluated by another investigator for different cases that we were working for approximately a month or so.

Various training that's come up over the years whether it be search warrant preparation, search warrant execution, various legal updates, things of that nature. Electronic data collection, examination, things like that.

Q So, now going to sort of the practical piece, have you obtained search warrants in the past?

A Yes, sir.

Q Okay. How many would you say? And if you can't estimate that, sort of what types of search warrants have you obtained?

A It would be hard to quantify that. Somewhere between 50 and 100 easily, I guess. So, social

media-type search warrants; Instagram, Facebook, live pings where we're trying to figure out where a suspect is or a subject is based on their cell phone location. Of course, the Google search warrants or geofence search warrants, search warrants involving DNA collection, tower dump search warrants, residential search warrants, vehicle search warrants, search warrants where I need to take a picture of a person's body that could have been a suspect of a rape or something of that nature. Historical-type search warrants.

Q Is that historical location?

A It could be historical location, that's correct.

Q Okay. Now, getting to the particular type of warrant in this case, a geofence warrant, have you obtained any geofence warrants in the past?

A I have.

Q How many prior to this case?

A Three prior to this investigation.

Q And were all of those signed by judges?

A Yes, sir.

Q Okay. What type? Was it federal or state?

A The first geofence warrant I acquired was actually in this district. The Honorable Judge David Novak, I believe. And then the two subsequent search warrants

were acquired by Chesterfield Circuit Court judges.

Q Okay. Now, prior to getting the search warrant in this case, did you consult with prosecutors about geofence warrants?

A With the prior warrants, yes.

Q What, if anything, did they tell you about the appropriateness of getting these types of warrants as a legal matter?

MS. KOENIG: Judge, objection. That is a legal conclusion which we have no witness to be able to testify about what advice was given, and that is not the appropriate question to be given in this case. This Court is to determine whether this warrant was valid.

MR. SIMON: Judge, it goes to the issue of good faith and, I think, hearsay as to what he was told or the advice that he's gotten about the propriety of these warrants is relevant.

THE COURT: Why don't you just ask one question in the negative? Have you ever been told it's not legal?

MR. SIMON: Okay.

BY MR. SIMON:

Q Have you ever been told it's not legal to get these?

A No, sir.
Q Now, the previous warrants that you obtained, these previous geofence warrants, were they substantially similar to the one you obtained in this case?
A They were mostly similar, that's correct. A few of them had more locations because of the more robberies to investigate.
Q Did they generally use the 150-meter radius?
A All but the search warrant that's sealed currently.
Q Okay. Now, prior to getting the search warrant in this case, did you receive any directive from leadership in your office at Chesterfield P.D.?
A I did, from my lieutenant and the courts.
Q Okay. What, if anything, did they tell you about where to go get your search warrant in this case?
A If possible, we would acquire our search warrants through a magistrate judge. Sorry. Not a magistrate judge, a Chesterfield County magistrate.
If for some reason a magistrate would not sign our warrants, we would schedule a meeting with an assistant commonwealth's attorney. We would speak with them about the matter and then try to schedule a time to see a circuit court judge.

Q Why at that directive?
A We were -- at the time we were overburdening the courts, and specifically the on-call judge. At least that was my understanding of it.
Q And that concern was coming from the Court?
A That's correct.
Q Okay. Now, was this the first geofence warrant in which you actually obtained the returns from Google?
A Yes.
Q Why hadn't you obtained the returns previously?
A Most of the incidents I was searching or working on prior to this particular geofence warrant weren't ones that were immediately concerning the public's welfare and safety.
Q Okay. But did you request the information back from them?
A Not in the same way that I did in this particular investigation. But yes, I submitted the search warrants, and I was awaiting a return.
Q Now, are you familiar at all with Google's internal practices about how they execute these warrants?
A No, sir, other than I submit them to Google, along with a nondisclosure order. They receive them and then process them however it is that they do that.

Q Now, there's been some discussion about cell phone dumps. Why didn't you get a cell tower dump in this case?

A It may have been an investigative technique that I would have done later, but in this particular instance, normally I reserve a tower dump search warrant for multiple crimes, multiple incidents, locations, things of that nature.

Q Okay. Now, let me -- before we get into the heart of the search warrant, can you explain for the Court what happened on May 20, 2019?

A Yes, sir. I was on duty or rather just got off duty, and I was informed by supervision that there was a bank robbery that had just occurred at the Call Federal Credit Union on Hull Street Road around the Genito area with a loss of approximately $195,000.

I came back on duty to respond out to the bank robbery as that was kind of my primary focus with Chesterfield at the time.

After my response to the scene, I interviewed witnesses, I reviewed surveillance camera video from both -- or at that time mostly just the Call Federal Credit Union Bank.

Through a culmination of all those investigative things that I had done at that point, I learned that a

suspect had come from the southwestern corner of the Journey Christian Church, which is a building adjacent and to the east of Call Federal Credit Union, at approximately 4:50 in the afternoon.

That same subject walked north in the parking lot, and then towards the front of the bank itself while holding what appeared to be like a cell phone to the side of his face or the side of his head.

That party then entered the bank, and we were able to get kind of a fuller shot of what he looked like. It was a black male. Witnesses described him, I think, in his twenties or thirties, approximately. Witness advised that he had a Jamaican accent, that he had kind of a scruffy beard and braided hair underneath of what was a round maybe fisherman's hat. He had reflective sunglasses and a reflective traffic vest.

He approached one teller while still having a cell phone up to the side of his face. He removes that cell phone, walks up to what we call a victim teller, presents a demand note. And I guess we can get into that further if you'd like.

But basically saying, I have your family as a hostage, your loved ones as a hostage outside. I have my -- I don't recall exactly how it says. But I know

people outside that have your family as hostage. If I see law enforcement responding, they may be hurt. You or your co-workers may be hurt.

The clerk advised the suspect, Hey, I don't have that much money. I don't have a $100,000 to give you. At which point he produces a silver or a black firearm and demands that all of the patrons and both employees of the bank come to the center area just as you enter.

He forced everyone to the ground kneeling or sitting, and, again, at gunpoint. Demanded who had access to the safe. The manager at the time advised that he did and kind of where the safe was located within the bank, which was in one of the back corners.

The suspect at that point stood everybody up, and, again, forced them all at gunpoint to the back of the bank where the safe was located, ultimately, again, putting everyone on the ground, and then forcing the manager at the time to open the bank's vault or safe. And then that's when he was able to take that money, the $195,000 that I spoke of, bank bands, insinuating, you know, what drawers and things that they came from.

Then, I believe, he collected a cell phone or two, and then started to exit, and then he kind of threw the cell phone devices somewhere within the business. And then kind of fled that same pattern around the

front of the bank and then back towards the southwestern corner of the Journey Christian Church.

Q Okay. What, if anything, did the phone trigger for you in terms of investigative techniques?

A For me, it meant that he could have possibly been speaking with a coconspirator. And then, obviously, for the purposes of the Google geofence warrant, that Google may have actually collected data that could have implicated him as being in the area at the time of the robbery.

In combination with the phone, possibly being on a phone call, and then the demand note to the victim teller, it told me that there was a possibility that he could have a lookout, that he could have a driver nearby or someone that was kind of keeping watch for law enforcement.

Q Okay. Now, prior to him entering the bank -- we've had some testimony. There was a witness who said they saw a suspicious blue Buick behind the sort of church area; right?

A Yes. That was an employee of the Journey Christian Church that was leaving somewhere between 4:30 and 4:40 in the afternoon.

Q Now, the geofence warrant in this case was obtained on June 14, 2019; right?

A Yes, approximately, like, three weeks or so after the robbery occurred.

Q Did you conduct any investigation in the interim?

A I did.

Q Did you get some leads?

A We did.

Q Okay. Tell the Court a little bit about that.

A I believe an estranged girlfriend or wife or whatever she was called in and basically said "I know who did this robbery. It's my ex-boyfriend." So, obviously, you know, he had some physical characteristics that were similar. He actually wore a fisherman style hat.

We were able to find him, interview him. I gave -- I believe I acquired a search warrant to acquire his cell phone device. We did some examinations on his phone. We found that he wasn't in the area at the time. He wasn't familiar with Call Federal Credit Union. He didn't frequent the area, even provided an alibi, I believe.

And we also had another party that one of the employees of a separate Call Federal Credit Union had brought to our attention that also had a blue Buick Lacrosse, I believe, and also came into a Richmond bank earlier that day wearing a traffic vest.

So my immediate concern at the time was this might be a likely suspect. We ran that to the ground as well. We were able to identify who that party was, and we were actually able to find that he was on an ankle monitor for, I believe, a crime that he committed in Richmond.

And then, of course, we were able to look at the GPS plots and data and see that he was nowhere near the Call Federal Credit Union in question today.

Q And you go and you get the geofence warrant sometime thereafter; right?

A That's correct.

Q I will show you what is marked as Government's Exhibit 2 and what's been admitted, and that's your search warrant; correct?

A Yes, sir.

Q That's your application?

A That's correct.

Q Now, when you submit this -- once you get the search warrant signed off by the magistrate, is it right that you submit -- what if we look at pages 4 and 5?

A Yes, that goes along with the search warrant.

Q Okay. And what else do you submit? Is it page 10?

A I'm sorry. The prior affidavits and 10 is going to be an attachment to the actual search warrant that's submitted to Google.

Q Okay. So if we look at -- I made a mistake. If we look at pages 4 and 5, we can put them next to each other and take a look. This is part of what you will submit to Google; right?

A Yes. Well, specifically, this is part of the affidavit to acquire the search warrant, but, yeah, there's data associated with this that also goes along with the search warrant attachment.

Q You don't actually submit what we will go through as the factual recitation of the case to Google; correct?

A No.

Q Okay. And the only other thing you submit in addition to pages 4 and 5 would be page 8, if we look at it; right?

A Yes, that's correct.

Q And just for purposes of the record, when I mention these page numbers, I'm talking about the red page numbering on Government's Exhibit 2.

A Yes.

Q Now, did you -- I just want to talk about the substance of what you provided to the magistrate in

getting this search warrant.

THE COURT: Wait a minute. The questions you were just asking him about are what went to Google?

MR. SIMON: Correct, Judge.

THE COURT: So just give me, again, the page numbers that went to Google, please.

BY MR. SIMON:

Q Pages 4 and 5, correct, Detective Hylton?

A The actual -- for me what was actually presented to Google would be page 8, page 10, and page 11 as far as in my affidavit and search warrant go.

Q Just to be clear, you're using the word "affidavit," but that's not -- you don't actually submit to them the probable cause.

A Yes, they don't get any probable cause narrative associated with the crime itself.

Q Okay. Now, looking at page 6, did you advise the magistrate of the note that the suspect left with the bank teller?

A Yes, sir.

Q Okay. Can we highlight that? You mentioned earlier that the note indicated that the suspect was potentially working with other people.

A Yes, sir.

Q Can you note for us where -- and it's highlighted

on the screen for you -- sort of where in there you got that inkling?

A Pretty much the first and second sentence. Would you like me to read it?

Q Sure.

A Okay. "I've been watching you for sometime now. I got your family as hostage and I know where you live, if you or your coworker alert the cops or anyone your family and you are going to be hurt. I got my boys on the lookout out side. The first cop car they see am going to start hurting everyone in sight, hand over all the cash. I need at least 100k and nobody will get hurt and your family will be set free. Think smartly. Everyone safety is depending and you and your coworkers action so I hope they don't try nothing stupid."

Q And did you also at the same time advise the magistrate that the suspected bank robber had a cellular telephone?

A Yes, sir.

Q Can we look at the paragraph starting "upon investigative response"?

A Yes.

Q Is this the paragraph in which you advise the magistrate about the cellular telephone?

A That's correct.
Q Can you go ahead and read some of this paragraph starting with the first few lines?
A Sure. Upon investigative response, law enforcement officials reviewed the bank's surveillance video prior to the robbery and noted the UNSUB, which is an unknown subject, had a cell phone in his right hand and appeared to be speaking with someone on the device. Subsequently, your affiant finds it necessary and prudent to request that Google provide geofencing data in order to assist with the investigation. In the undersigned's training and experience, when people act in concert with one another to commit a crime, they frequently utilize cellular telephones and other such electronic devices, to communicate with each other through Wi-Fi, Bluetooth, GPS, voice calls, text messages, social media accounts, applications, emails, and/or cell towers in the area of victim-businesses, and in this case, located at 3640 Call Federal Drive, Chesterfield, Virginia 23235. Furthermore, the requested data/information would have been captured by Google during the requested time.
Q Okay. And if we go to page 7, did you then advise the magistrate about Google location information, Google accounts, and cellular telephones, a bit more

information there?
A Yes, sir.
Q If we look at the second paragraph, is that one of the places in which you tie the fact that Google -- that folks can have Google accounts on their cellular telephones?
A Yes, sir, that's correct.
Q And then if we look at paragraph 3, as well.
A Yes, sir, that's correct, as well.
Q Now, in addition to -- in this particular paragraph, paragraph 3 on page 7, notes Android phones as a place where Google accounts might be included. Did you also advise the magistrate that Google accounts could be on non-Android phones?
A That's correct, through applications of similar sorts.
Q Now, did you tie the fact that Google location information -- or Google accounts are on phones, but did you also tie the fact that Google collects location information from these phones?
A Yes, sir.
Q If we look at paragraphs 4 and 6, and I think we'll have to look at them one at a time. Look at paragraph 4 here. Is this one of the paragraphs in which you advised -- in which you advise the Court

that Google location information could be captured by cellular telephones?

A Yes, sir, that's correct.

Q Now, looking at paragraph 6 on page 7 of Government's Exhibit 2, is this another paragraph in which you noted to the magistrate why location information might be on a cellular telephone?

A That's correct.

Q And why that -- and noted that that location information is tied to a Google account?

A Yes, that's correct.

Q Now, have you in your personal experience ever encountered a situation set forth in paragraph 6 there using images or videos on a cellular telephone to solve a crime?

A Yes, sir.

Q Can you tell us about that?

A Sure. In a few instances that I've investigated crimes, I've had an abduction at gunpoint, knifepoint, where a subject was carjacked and then taken to the place of a robbery. When we ended up developing a lead or a target in that particular investigation, we were able to gain probable cause, conduct a Facebook search warrant for his data, and he actually had multiple GPS plots showing that he was in the area of

the robbery, and actually posting pictures and things of that nature associated with the robbery in the general area of the parking lot of the business that was robbed.

And similar type instances where I've worked other robberies where suspects have had metadata associated with an image or even video prior to and after a robbery where he's taking pictures of himself, flashing money subsequent to the robbery, or flashing a firearm and even a mask prior to actually committing a robbery.

MR. SIMON: Judge, I've got a few more questions, probably two or three, I think.

BY MR. SIMON:

Q With respect to this pervasiveness of cell phones in American society, did you set that forth in paragraph 7 of this on page 7?

A Yes, sir.

Q Is that the Pew Research study set forth there?

A That's correct. Although, it was likely dated at the time as that was September 2013.

Q In addition to the fact that all of this information is out there, and we talked about paragraph 6, but did you also in paragraph 5 explain for the magistrate how this information would be

helpful in terms of locating an individual?
A Yes, that's correct.
Q Can we highlight paragraph 5 here. Can you read that?
A Sure. "This applicant knows that location data can assist investigators in forming a fuller geospatial understanding and timeline related to a specific criminal investigation and may tend to identify potential witnesses and/or suspects. Such information can also aid investigators in possibly inculpating or exculpating persons of interest."
Q So that paragraph notes the potential interest in witnesses as well?
A That's correct.
Q Again, this affidavit, pages 6 and 7, that we just went through, Google had no knowledge of these facts; correct?
A That's correct.
Q And it's typical practice not to give these companies the actual facts of the case; right?
A That's correct.
Q Now, I'm just going to end with quickly showing you Government's Exhibit 4. It's a number of pages there. Just take a look at them. Do you recognize the pages in Government's Exhibit 4?

A Yes.
Q What are those?
A These are correspondence between myself and Google through email.
Q Okay. And that's an accurate reflection of those emails?
A Yes, sir.

MR. SIMON: Judge, we move to admit and publish briefly these emails.

MS. KOENIG: No objection.

THE COURT: All right. They'll be entered.

(Government's Exhibit No. 4 is admitted into evidence.)

BY MR. SIMON:
Q Now, let me ask you just some quick questions here. The emails that were sent to Google, was there a fair amount of follow-up via email?
A No, I don't believe any except for the receipt of the stages during the process.
Q Okay. And so when you talked with -- Sarah Rodriguez mentioned that at some point you talked with someone from Google on July 8. Did you initiate that communication?
A I did, but I believe I called twice.
Q Why did you call on July 8?

A It was either to receive the first or to try to receive Stage 1 at a faster rate of speed due to the exigency of the suspect posing a danger to the public and then also being a possible flight risk.

Q The July 8 communications, that came after you received the first round; right?

A Yes, that's correct.

Q So when you called on July 8, you were trying to get the second round of information?

A Correct.

Q And prior to that you had sent two emails; correct?

A Yes.

Q And had received no communication from Google?

A That's correct.

Q Throughout these emails, did you tell anything to Google about the dangerousness of the situation?

A I did.

Q And these emails were sent in consultation with my office; right?

A That's correct.

THE COURT: Consultation with whom?

MR. SIMON: Consultation with my office.

THE COURT: Okay.

MR. SIMON: No further questions, Judge.

THE COURT: Is there cross?

MS. KOENIG: Yes, sir.

MR. SIMON: Judge, I think I moved Exhibit 4 in already.

THE COURT: You did.

CROSS-EXAMINATION

BY MS. KOENIG:

Q Good evening, Detective.

A Good evening.

Q I want to start with the surveillance videos. So you looked, as a part of the investigation, at the widest surveillance videos that the bank had provided; right?

A That's correct.

Q And you looked at those before June 14th of 2019?

A Yes, ma'am.

Q And those surveillance videos include outside areas of the bank; right?

A That's correct.

Q And you also looked at the church surveillance videos; right?

A Yes, ma'am.

Q And the church surveillance videos include directions that face from the church toward the bank; right?

A That's correct.
Q And include wide swaths of that parking area; right?
A Yes, ma'am.
Q I want to make sure, you had looked at that before you filed for this warrant on June 14th of 2019; right?
A I believe so.
Q And you also had a witness that was at the church; right?
A Yes, ma'am.
Q And that witness said that that person saw -- that that witness saw one individual walking toward a blue Buick; right?
A No, ma'am. One individual inside of a blue Buick.
Q I'm sorry. And did they provide a description of the person that was inside of the vehicle?
A That description changed in three different interviews with that individual. I believe the initial was a black male. Then, I think, it became a person or a male. And then I don't recall what the last interview was.
Q All right. When you watched the bank surveillance videos, you saw no one else that you could not account for except for the suspect in the fisherman's hat and

the traffic vest; right?
A Yes, ma'am, that's correct.
Q And when you watched the church surveillance videos, you saw no one else that you could not account for except for the suspect in the fisherman's hat and the traffic vest; right?
A That's correct.
Q You did not put those details in your affidavit to the magistrate; right?
A No, ma'am. If they're not in there individually, they're not in there.
Q All right. In going to your statement --
A Actually, ma'am, I do apologize. I did mention, I believe, in a part of my affidavit where a suspicious subject was seen parked behind the southwestern corner of the church.
Q Sure, but you didn't mention that you hadn't -- you had seen surveillance video and you had not seen any other possible codefendants on the surveillance video.
A That's correct. No other codefendants were seen.
Q All right. And you also didn't see any hostages being held anywhere outside of the bank; right?
A No, ma'am.
Q I want to make sure I heard. How many -- before

June 14 of 2019, how many geofence warrants had you applied for?

A Three.

Q One is a search warrant from April 11 of 2019 in Chesterfield County; right?

A That's correct.

Q One is a federal search warrant from February 22, 2019, from this courthouse, Judge Novak?

A That's correct.

Q What is the third one?

A The third one is the one that's under seal. It's a homicide investigation. It was also obtained in April, but I -- did you say the first was obtained on the 8th or April 8th?

Q April 11.

A April 11. I believe the other is actually April 8.

MS. KOENIG: Your Honor, I don't mean to belabor this point. We have asked ad nauseam for these warrants. I have asked several times. I have emails from Mr. Simon that indicate that the only two warrants that he had applied for before were the state search warrant that I have identified on April 11 of 2019 and the federal search warrant. I do not have a copy of any third search warrant, and I'm asking for

that yet again.

MR. SIMON: Judge, we've given every search warrant that we can get access to in this case. I also would have to look at the briefs. I'm pretty sure we indicated three. I don't want to say anything that's wrong.

What I can tell you is that I know I can't get access to the third. That's an ongoing homicide investigation. And the ACA there certainly is not inclined to unseal that. That's my understanding. And so that's sort of the fullest extent that I can get into that. But, as I've noted, we've given everything that we have.

THE COURT: All right. I'm going to allow you all to brief that up later based on the record that you can establish. Five pages each.

THE WITNESS: If I can, ma'am. That matter hasn't even come up in court yet. It's actually scheduled to be January of 2022.

BY MS. KOENIG:

Q All right. So let's go back to your training and experience. You have not received any specific training about geofence warrants; right?

A No, ma'am, I have not.

Q And you've not received any training specific to

how to request geofence warrants; right?
A No, ma'am.
Q You learned about geofence warrants through other police officers that you work with; right?
A That's correct.
Q All right. So let's look at Defense Exhibit -- I'm sorry. If we could pull up Government's Exhibit 2, please. Thank you. All right. Government's Exhibit 2 is the geofence warrant in this case; right?
A Yes, ma'am.
Q All right. So let's look at Attachment 1, which is on page 3. And if you can flip in the defense exhibit book to Defense Exhibit 19, please.
A I apologize.
Q It is the big one.
A You said 19, ma'am?
Q Yes. I'll just kind of save you a little bit of time.
A I'd appreciate it.
Q Absolutely. So that exhibit comprises two warrants. If you'll see that there's a warrant -- I'll wait until you get there.
THE COURT: I'm not there yet either.
MS. KOENIG: Sorry, Your Honor.
BY MS. KOENIG:

Q All right. So would you agree with me that that exhibit contains two warrants, one of which has the warrant -- the affidavit file number of 42 at the beginning?
A Yes, ma'am.
Q And then the subsequent pages to that are related to that warrant; right?
A That's correct.
Q And then the second warrant is affidavit file No. 472; right?
A Are we speaking of my search warrant at this point?
Q That's correct.
A That's correct.
Q So that's 472 is your search warrant; right? You can look at it.
A Yes, ma'am.
Q So look at Attachment 1 from the geofence warrant in this case. Just keep your page. Don't change the page.
A Sorry.
Q That's okay. So I want you to compare Attachment 1 from Government's Exhibit 2 to Attachment 1 in the affidavit that you filed in file No. 472.
A So, just to clarify, Detective Humphries

Attachment 1 versus my Attachment 1.
Q Correct. Let's just make this easier. Detective Humphries filed for the affidavit in search warrant number -- the affidavit file No. 42; right?
A Correct.
Q Detective Humphries is somebody that you work with at the Chesterfield County Police Department; right?
A Yes, that's correct.
Q All right. So, again, let's look at the Attachment 1 from Government's Exhibit 2 and compare that to Attachment 1 in file No. 472, which is the second warrant in Exhibit 19.
A Yes, ma'am.
Q Those are the same; right?
A As far as I can see, they're pretty much the same.
Q While we're on Attachment 1, let's look at file No. 42, which is the first warrant, Defense Exhibit 19.
A Okay.
Q So when you look at Attachment 1 -- Attachment 1, go to Detective Humphries --
A Yes, I'm on Detective Humphries'.
Q Okay. Attachment 1 in Detective Humphries' affidavit, which is file No. 42, is also the same as the search warrant Attachment 1 in this geofence

warrant case, in our case; right?
A Yes, ma'am.
Q All right. Let's go to Attachment 2 of Government's Exhibit 2. All right.
So Government's Exhibit 2, Attachment 2, please compare that to your search warrant in file No. 472, which you got, which is the second warrant, that's in Defense Exhibit 19.
A Without directing looking at them, I believe it's going to be the same since I'm the one that filed it, or, sorry, I'm the one that acquired it.
Q And the only thing that's different, right, is the date and time?
A Correct.
Q The crime that is associated and the geographic area to be searched; right?
A That's right.
Q So let's compare Government Exhibit 2, Attachment 2, to Detective Humphries' Attachment 2 in file No. 42.
A Okay.
Q And, again, the only substantive changes, right, are the date and time that applies and the geographic location; right?
A Yes, ma'am. And then the way that the --

Q There's a little formatting change; right?
A Correct.
Q All right. So you did not draft either Attachment 1 or Attachment 2 for your June 14, 2019 warrant in this case; right?
A Not solely by myself, no.
Q Okay. And you mentioned already that you had applied for a --
MS. KOENIG: Judge, I move to admit Defense Exhibit 19?
THE COURT: Any objection?
MR. SIMON: Judge, I would object to it being entered into the record. I think it's fairly clear he's using a go by, but I don't know why we'd want a different detective's search warrant in this particular record. It has nothing to do with this case or the probable cause in his warrant.
THE COURT: Well, she's using it to say it's the same language. So she's acknowledging they're different things.
MR. SIMON: Okay.
THE COURT: So that's overruled.
(Defense Exhibit No. 19 is admitted into evidence.)
BY MS. KOENIG:

Q And I forgot to ask you, Detective, although it is apparent from the face of the application --

THE COURT: You are talking to your computer.

MS. KOENIG: Thank you.

BY MS. KOENIG:

Q I forgot to ask you, did file No. 42 that Detective Humphries got --

A Yes.

Q He got that affidavit -- he filed for that search warrant on January 8 of 2019; right?

A Yes, ma'am.

Q All right. So, let's turn -- you mentioned a federal search warrant. The federal search warrant is -- let's look at Defense Exhibit 18.

A Are we still going to be using mine as a reference, as well?

Q We are. You know where I'm going.

A All right. Go ahead.

Q So this is the federal search warrant that you applied for; right?

A Yes, ma'am.

Q All right. And you got this warrant on February 22, 2019?

A Uh-huh.

Q And that's a yes or a no?

A Yes, ma'am. Sorry.
Q That's okay. Let's look at Attachment A of the federal warrant. It's ECF page No. 20 at the top.
A Page 20?
Q Yes.
A All right. Thank you.
Q So when we are looking at Attachment A and comparing Attachment A -- so Attachment A is the property to be searched; right?
A Yes, ma'am.
Q All right. And that is a similar purpose for Attachment 1 in Government's Exhibit 2; right?
A That's correct.
Q All right. The language varies dramatically; right?
A Somewhat, and that's mostly actually due to the structure of the federal warrant versus the state search warrant.
Q Sure. Well, aside from -- the only thing that actually is the same in terms of the language is the place where Google accepts legal process in Mountain View, California; right?
A That's correct. And that's actually listed in a different place in my affidavit and search warrant.
Q That's fine. So, then we get locations A through

O on that page; right?
A Yes.
Q And you put together locations A through O; right?
A I did.
Q You did not draft that paragraph above the locations A through 0; right?
A No, I didn't specifically -- that was kind of the go by situation that we were referring to earlier.
Q All right. So, let's go to Attachment B in Defense Exhibit 18, and that starts on page 31 of the ECF at the top of that exhibit.
A Okay.
Q All right. So, again, we're going to compare. So Attachment B in Defense Exhibit 18 is items to be seized and searched; right?
A Yes, that's correct.
Q And the purpose of that attachment is similar to the purpose of Attachment 2 of Government's Exhibit 2; right?
A Yes, ma'am.
Q All right. And that outlines the three-step process -- Attachment B sets out the three-step process that Google created for geofence warrants?
A Yes, ma'am.
Q So when we compare Attachment B in Defense Exhibit

18 to Attachment 2 in Government's Exhibit 2, those are different; right?

A Yes, ma'am, slightly different.

Q Slightly?

A Well, in the way that they're laid out, but the information that I'm seeking is still the same.

Q But there's not a single sentence in Attachment B in Defense Exhibit 18 that is the same as Attachment 2 in Government's Exhibit 2; right? You can take your time.

A Okay.

Not on this particular page I'm looking through right now.

Q It's a pretty short second page.

A That's correct.

Q And you also didn't write Attachment B to the federal search warrant; right?

A As in come up with the language myself? No, ma'am.

Q Correct. Thank you.

MS. KOENIG: I move to admit Defense Exhibit 18, Your Honor.

MR. SIMON: No objection, Judge.

THE COURT: It will be entered.

(Defense Exhibit No. 18 is admitted into

evidence.)

BY MS. KOENIG:

Q When you were putting together the geofence warrant in this case in Government's Exhibit 2, you did not have a suspect; right? You had a body. You didn't have any individual person; right?

A That's correct. I did not have a name attached to the suspect at that time.

Q All right. And the only way you gained the suspect in this case was through the geofence warrant; right?

A In this particular instance, yes.

Q And you ultimately identified Okello Chatrie as a suspect in this case?

A I did.

Q And you investigated Mr. Chatrie's background?

A Yes, ma'am.

Q You knew he was Jamaican?

A I did.

Q You knew he came to the United States from Jamaica in 2017?

A That's correct?

THE COURT: You are --

MS. KOENIG: I'm sorry, Your Honor.

BY MS. KOENIG:

Q Let's talk now about when you presented the affidavit that you assembled in Government's Exhibit 2 to the magistrate.
A Okay.
Q You went to Magistrate David Bishop; right?
A That's correct.
Q Did you know that Mr. Bishop had never before issued a geofence warrant?
A I did not.
Q Was he the only magistrate on duty when you presented him with a geofence warrant application in the case?
A It's been a while. Normally, they have two or three on duty.
Q How did you present it to him?
A In the way that it's kind of seen here.
Q I'm sorry. Maybe I'll be more specific. How did you physically present it to him? Did you just hand it to him?
A Yes, ma'am. I walk up to him. I hand him the affidavit. I sign it in front of him. I swear. Then he takes that paperwork, and he reviews it himself, and then decides if there's probable cause based on what he's reading in the four corners of the actual affidavit itself.

Q Did Mr. Bishop ask you any questions about the contents of the application?
A I don't recall any questions asked.
Q Did he seek to modify anything in the affidavit at all?
A No, ma'am.
Q Did he just read it and sign it?
A That's my understanding. He could have consulted with someone. I wasn't sure.
Q Did he read it in front of you?
A I don't believe so.
Q How long did it take?
A I don't know. It's been 2019. I couldn't advise.
Q More than 15 minutes?
A I would assume so.
Q More than 30 minutes?
A I don't know. I'm sorry.
Q All right. So, going back to the --

MS. KOENIG: Let's see if we can switch screens to the government's screen, Ms. Hancock.

BY MS. KOENIG:
Q So going back to Attachment 2 of Government's Exhibit 2, which is page 5, on the second page or on that page, second page of Attachment 2, there is a picture; right?

A Yes, ma'am.
Q And that is the geofence itself; right?
A That's correct.
Q And so you have a description of that area above the picture; right?
A Yes.
Q And that description says, "An area encompassing the Call Federal Credit Union and an adjacent business"; right?
A Yes.
Q That adjacent business you're referring to is the Journey Christian Church?
A That's correct.
Q And that's the much larger building to the right of the credit union in the picture that we're looking at?
A That's correct.
Q And so you've obviously been a detective in Chesterfield for a little while; right?
A Yes, ma'am.
Q And you went to the bank the day of the robbery; right?
A I did.
Q You knew it was the Journey Christian Church next door; right?

A Yes, ma'am.
Q And you knew that the Journey Christian Church is what we would call a mega church?
A It was a church within a --
Q It's a very large church.
A Yes, it's a large building, but it's actually an old Costco or something to that nature.
Q Sure. And you know a lot of people attend that church; right?
A No, ma'am.
Q You don't know that?
A I don't know any person to my knowledge that goes to that church.
Q All right. Let's talk about the time frame for the execution of the warrant. So if we can look at Government's Exhibit 4. I guess I can pull it up on mine. Let me do that. All right. So you submit -- are you there?
A Yes, ma'am.
Q Okay. So page 1. You submit -- you get the warrant on June 14, 2019; right?
A That's correct.
Q You submit it to Google on June 20, 2019; right?
A Yes.
Q You sent some follow-up information to Google on

June 25, 2019; right?
A Yes.
Q And Google provides you the Stage 1 response on June 28, 2019?
A That's correct.
Q And in the Stage 1 response, you get the location data on the 19 devices?
A Yes.
Q And then on July 1, 2019, you make the first Stage 2 request?
A That's right.
Q On July 2, you make a second Stage 2 request?
A Yes, ma'am.
Q And on July 8, you make a third Stage 2 request; right?
A Yes, that's correct.
Q And then after you make that email request on July 8, 2019, that's when you leave the two messages for the LIS specialist at Google; right?
A Yes, ma'am.
Q And that person calls you later that day; right?
A They did.
Q All right. So then July 9 is when you narrow down the Stage 2 request to nine devices?
A That's correct.

Q And you get the second stage return on the same day?
A Yes, ma'am. Looks that way.
Q And then July 10, you make the Stage 3 request?
A Yes.
Q And then July 11, you email again asking for the Stage 3 data?
A Yes.
Q And then July 11, you get the Stage 3 data?
A That's correct.
Q All right. So I want to talk to you about search warrant returns.
A Okay.
Q The purpose of a -- well, a search warrant return is a document that notifies the Court when you execute the search warrant; right?
A Yes, ma'am.
Q When you execute a geofence search warrant, it's executed when you send it to Google; right?
A That's correct.
Q And you send it via the LER system; right?
A Yes, ma'am, the L-E-R system, yes.
Q And in return, you also report -- in the return, you also report back to the Court what items you gathered during the search; right?

A That's correct.
Q All right. So let's look at Government's Exhibit 2, which I will pull up on the screen. No, I don't have it. Government's Exhibit 2 on page 9.
MS. KOENIG: Ms. Hancock, if we could ask, if we could get the government's screen, that would be great. All right. Thank you very much.
BY MS. KOENIG:
Q So we are looking on page 9 of Government's Exhibit 2 at the "search inventory and return" on this case; right?
A Yes, ma'am.
Q So, in the execution part on the right-hand side, you indicate that the search warrant was executed on July 14, 2019, at 10:30 in the morning.
A That's correct.
Q And that's not true; right?
A That's correct, not when it was forwarded to Google, that's correct.
Q And we just discussed that when you forward it to Google, that is the execution of the warrant; right?
A Yes, ma'am, that's when Google receives the warrant.
Q All right. You filed this return on June 19 of 2019; right?

A Yes, ma'am, that's when it was submitted physically to Google through the LERS website.

Q Well, we'll come back to that in a second.

So, in the bottom half of the search inventory and return, there's a portion that has your signature. I'm assuming that's right above executing officer?

A Yes.

Q It's about the same as my signature. I'll tell you, I'm not going to give you grief about that.

And then the date is June 19th of 2019; right?

A That's correct.

Q And the statement above that says, "The statement above is true and accurate to the best of my knowledge and belief"; right?

A Yes, ma'am.

Q And you indicate that what you had received and seized pursuant to this warrant is data; right?

A That's correct.

Q All right. So this is June 19th of 2019. When we go to Government's Exhibit 4 at page 1, you do not submit the Google -- the geofence warrant in this case to Google until June 20th, the day after you file a return; right?

A Yes, ma'am, that's correct. This is their response to having received it in the LERS program.

Q And you also don't receive any data, even the Stage 1 data, until June 28th of 2019; right?
A That's correct. Sounds correct.
Q And then you don't receive the final Stage 3 data, which is ultimately what you're seeking, until July 3? I'm sorry. July 11 of 2019?
A That's the Stage 3 data?
Q Yes.
A Yes, ma'am, that's correct.

MS. KOENIG: No further questions.

MR. SIMON: Judge, I just want to put on the record something about the sealed search warrant.

THE COURT: Okay. So there's no further questions?

MR. SIMON: A question.

THE COURT: All right. It's going to be a couple minutes, because we're about two minutes away from one hour.

MR. SIMON: Judge, I think it might literally take three minutes.

THE COURT: All right.

REDIRECT EXAMINATION

BY MR. SIMON:

Q Detective Hylton, the search warrant that's under seal, did you seek to get that record from the

Assistant Commonwealth's Attorney?
A I believe I did.
Q And what, if anything, did he tell you about whether he wanted keep that search warrant sealed?
A She. And she told me no, it was sealed.
Q And that she wanted to keep it sealed; correct?
A That's correct.
MR. SIMON: No further questions, Judge.
THE COURT: All right. Can this witness be excused?
MS. KOENIG: From the defense' perspective, yes, Your Honor.
MR. SIMON: From the United States, yes.
THE COURT: All right. You may be excused, sir.
(The witness was excused from the witness stand.)
THE COURT: So there's no further evidence; am I right?
MR. SIMON: No further evidence, Judge.
THE COURT: So this is what we're going to do. We're going to take a recess. I'm going to have you guys talk about what the next process is. I presume you're going to order a transcript. So I want you to sort of talk about that, and then hopefully not

very long we'll put something on the record.

If y'all need time to talk about, you know, the five-page submission about the sealed warrant, fit that in. If you think you can't get it done tonight because folks are too blurry eyed, we can do something, I guess, by ZOOM on Monday as far as scheduling. But I want to try to close this up, realistically, as far as what the next steps will be. All right?

MR. SIMON: Understood, Judge.

THE COURT: Okay. So we're going to take a brief recess.

Thank you, Officer Hylton. I did that late. Thank you for your testimony.

OFFICER HYLTON: Yes, ma'am.

(Recess taken 7:15 p.m. until 7:27 p.m.)

THE COURT: All right. What are our logistics?

MS. KOENIG: Your Honor, we've spoken with Ms. Daffron, who's let us know when the transcript can be ready, and based on that, we would request that by April 30th the defense submit a supplemental motion to suppress that addresses the legal issues on the basis of the facts and evidence presented.

The government would file their response on

May 21st. And then the defense would file a reply on June 4.

In terms of the state search warrant that Detective Hylton discussed that's under seal, the understanding is that the government -- or my understanding is that the government is going to review -- because my question is whether or not Attachments 1 and 2 in that warrant are different than what is in Government's Exhibit 2. And so they are going to review that and get back to us, and if we have any further issues past that, I'll let you know.

THE COURT: Okay.

MS. KOENIG: I think that addresses the issues. And I've spoken with Ms. Hancock. Instead of keeping everyone here tonight to sort out exhibits, we'll sort them out next week.

THE COURT: No, I think that makes great sense.

So we'll issue that order with respect to briefing. If you all want to schedule just an argument after that, we can also consider that date, so that's on the record at the same time. And I don't know if you all will want that argument. I presume you might actually. Right?

MS. KOENIG: I'm sorry.

THE COURT: Will you want argument?

MS. KOENIG: Yes.

THE COURT: Let me see if I have a calendar. I know I have a calendar because I asked my clerk for one, but that was a whole day ago.

How about we call you about potential argument dates, and that will be in the order at the same time. All right?

MS. KOENIG: Yes, Your Honor. Thank you.

THE COURT: That way I can check my record.

And let me ask, this is just on these motions. You're going to rest on the motions that we have as to the houses and the other materials?

MS. KOENIG: We'll wait until the Court resolves this motion, I think, before we need to resolve those.

THE COURT: Okay. So they will just remain in place pending, and we will -- obviously, this precedes all of that.

MS. KOENIG: That's right.

THE COURT: All right. So I appreciate your efforts. I do think it will be worth going through the exhibits. I have taken notes, and we have, and it's important that we get the record exactly the way we want it to be, including not just substituting your

43A, Ms. Koenig, but also substituting the documents that we excised pages out of.

MS. KOENIG: That's right.

THE COURT: So that we have just one full record, and that everybody is agreeing upon what we have. All right?

MR. SIMON: Understood, Judge.

THE COURT: So, Mr. Chatrie, I apologize that we go through these proceedings and talk about you in the third person the whole time, but I want you to know that obviously we're doing that because that's how it's supposed to work. Your attorneys are speaking on your behalf, and I can see that you have been engaged exactly as you should be during this process. And I want to be sure that you stay in close contact with your attorneys so that you can ask them any questions about what's going forward.

They have been very good about letting me know anything that they think needs to be addressed, either they think themselves and/or you want them to say that. So I definitely want you to continue to be engaged in that process.

And I appreciate everybody's hard work. I appreciate everybody who had to stay late. I think it's better to finish tonight, but I am aware, for

instance, Mr. Chatrie, you still have a drive, which means other folks are driving with you. So I just please ask, be safe, and thank you for your good work. All right?

THE DEFENDANT: Thank you, Your Honor.

(The proceedings were adjourned at 7:30 p.m.)

I, Diane J. Daffron, certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/s/

_____ _____

DIANE J. DAFFRON, RPR, CCR DATE

This page intentionally left blank for double-sided pagination and printing

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Richmond Division (The Hon. M. Hannah Lauck)

JOINT APPENDIX

VOLUME 5 of 11 (pages 1071 - 1326)

JESSICA D. ABER
United States Attorney

Kenneth R. Simon, Jr., Ass't U.S. Attorney
Peter S. Duffey, Ass't U.S. Attorney
Counsel for Appellee
919 East Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400

Nathan P. Judish, Senior Counsel
Computer Crime & Intel. Property Section
Criminal Division
U.S. Department of Justice

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
Counsel for Appellant
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800

Michael W. Price, Litigation Dir.
NACDL Fourth Amendment Ctr.
1660 L Street NW, 12th Floor
Washington, DC 20036

This page intentionally left blank for double-sided pagination and printing

TABLE OF CONTENTS

VOLUME 1 (pages 1 - 176)

District Court Docket Sheet (as of Jan. 17, 2023) 1

Indictment (Sept. 17, 2019, Doc. 1) 22

Defendant's Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Oct. 29, 2019, Doc. 29) 25

Government's Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (Nov. 19, 2019, Doc. 41) 51

Defendant's Reply to Government's Response [to] Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Dec. 9, 2019, Doc. 48) 76

Exh. A (First Step 2 Request to Google) (Doc. 48-1) 98
Exh. B (Second Step 2 Request to Google) (Doc. 48-2) 100
Exh. C (Third Step 2 Request to Google) (Doc. 48-3) 102
Exh. D (Transcript, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019)) (Doc. 48-4) ..... omitted from J.A.

Government's Notice Regarding Attachment of Google Geofence State Search Warrant to Response in Opposition to Motion to Suppress (Dec. 18, 2019, Doc. 54) 104

Affidavit for search warrant and warrant, with attachments (Doc. 54-1) 107

Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant (Dec. 20, 2019, Doc. 59-1) 118

United States' Response to Amicus Curiae Brief of Google LLC (Jan. 10, 2020, Doc. 71) 148

Defendant's Response to Google's Motion to File Amicus Curiae Brief in Support of Neither Party (Jan. 10, 2020, Doc. 72) 158

VOLUME 2 (pages 177 - 416)

Transcript, Discovery Motion Hearing (Jan. 21, 2020, Doc. 81; *see* Doc. 77 (court minutes))....177

Preliminary matters....179

Def't witness Spencer McInvaille — Direct examination....193; Cross examination....283; Redirect examination....306

Argument by the defense....318
Argument by the government....332
Rebuttal by the defense....350

Court's ruling....355

Defendant's Supplemental Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (May 22, 2020, Doc. 104)....363

United States' Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (June 12, 2020, Doc. 109)....393

VOLUME 3 (pages 417 - 694)

Transcript, Suppression Motion Hearing, Day 1 (evidence) (Mar. 4, 2021, Doc. 201; *see* Doc. 198 (court minutes))....417

Preliminary matters....420

Def't witness Spencer McInvaille — Direct examination....432; Cross examination....542; Redirect examination....586

Def't witness Marlo McGriff — Direct examination....606

VOLUME 4 (pages 695 - 1070)

Transcript, Suppression Motion Hearing, Day 2 (evidence) (Mar. 5, 2021, Doc. 202; *see* Doc. 199 (court minutes)) 695

Preliminary matters 698

Def't witness Marlo McGriff, cont'd — Direct examination ..... 699; Cross examination ..... 791; Redirect examination 841

Def't witness Sarah Rodriguez — Direct examination ..... 862; Cross examination ..... 902; Redirect examination 916

Gov't witness Jeremy D'Errico — Direct examination ..... 923; Cross examination ..... 967; Redirect examination 1010

Gov't witness Joshua Hylton — Direct examination ..... 1016; Cross examination ..... 1040; Redirect examination 1063

Concluding matters 1064

VOLUME 5 (pages 1071 - 1326)

Defendant's Post-Hearing Brief on "Geofence" General Warrant (May 3, 2021, Doc. 205) 1071

Government's Response in Opposition to Defendant's Motion for Suppression (May 21, 2020, Doc. 214; *see* Doc. 207-2) 1117

Defendant's Reply to Government's Response in Opposition to Motion for Suppression (June 4, 2020, Doc. 213) 1164

Transcript, Suppression Hearing (arguments) (June 24, 2021, Doc. 217; *see* Doc. 215 (court minutes)) 1185

Argument by the defense 1187
Argument by the government 1231
Rebuttal by the defense 1313

Concluding matters 1322

VOLUME 6 (pages 1327 - 1456)

Memorandum Opinion (denying suppression motion) (Mar. 3, 2022, Doc. 220) 1327

Order (denying suppression motion) (Mar. 3, 2022, Doc. 221) 1390

Criminal Information (May 6, 2022, Doc. 224) 1391

Transcript, Change of Plea Hearing (May 9, 2022, Doc. 247; *see* Doc. 226) 1394

Plea Agreement (May 9, 2022, Doc. 228) 1428

Statement of Facts (May 9, 2022, Doc. 229) 1444

Judgment in a Criminal Case (Aug. 19, 2022, Doc. 239) 1449

Notice of Appeal (Aug. 25, 2022, Doc. 241) 1456

VOLUME 7 (pages 1457 - 1810) – DOCUMENT EXHIBITS

Exhibits Admitted at Discovery Motion Hearing (Jan. 21, 2020)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) ..... *see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) ..... *see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) ..... *see* J.A. 2093
Def't Exh. 4: Activation Video ..... omitted from J.A., available on request
Def't Exh. 5: Three Paths Video (sealed) ..... *see* J.A. 2139
Def't Exh. 6: First Step 2 Request to Google 1457
Def't Exh. 7: Second Step 2 Request to Google 1459
Def't Exh. 8: Third Step 2 Request to Google 1461

Def't Exh. 9: Step 3 Request to Google 1463

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) .....*see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) .....*see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) .....*see* J.A. 2093
Def't Exh. 5: Three Paths Video (sealed) .....*see* J.A. 2139
Def't Exh. 6: Spencer McInvaille Report 1464
Def't Exh. 7: Spencer McInvaille Supplemental Report 1469
Def't Exh. 8: CSV Google Data File (.csv file) .....*see* J.A. 2139
Def't Exh. 9: Unique in Crowd Study 1475
Def't Exh. 11: September 2018 Oracle Submission 1480
Def't Exh. 18: Federal Search Warrant Application & Attachments 1502
Def't Exh. 19: State Search Warrants & Attachments 1534
Def't Exh. 21: McGriff Declaration 1 (Doc. 96-1) 1551
Def't Exh. 23: McGriff Declaration 3 (Doc. 147) 1562
Def't Exh. 24: Rodriguez Declaration (Doc. 96-2) 1579
Def't Exh. 27: Every Step You Take 1587
Def't Exh. 30: AZ Ex. 18 (admitted portions only) 1631
Def't Exh. 31: AZ Ex. 19 (admitted portions only) 1633
Def't Exh. 32: AZ Ex. 20 1639
Def't Exh. 33: AZ Ex. 24 1644
Def't Exh. 34: AZ Ex. 202 1667
Def't Exh. 36: AZ Ex. 209 1777
Def't Exh. 38: AZ Ex. 219 1781
Def't Exh. 40: AZ Ex. 236 1797
Def't Exh. 41: AZ Ex. 260 1804

VOLUME 8 (pages 1811 - 2090) – DOCUMENT EXHIBITS, CONT'D

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021), cont'd

Def't Exh. 43: May 2018 Privacy Policy – Redline 1811
Def't Exh. 43a: May 2018 Privacy Policy – Redline (with internet source information) 1840
Def't Exh. 44: Jan. 2019 Privacy Policy – Redline 1865
Def't Exh. 45: Oct. 2019 Privacy Policy – Redline 1895
Def't Exh. 46: McGriff Blog 1 1926

Def't Exh. 47: McGriff Blog 2 1929
Def't Exh. 48: 2018 Quartz Article 1934
Def't Exh. 49: 2018 AP Article 1 1941
Def't Exh. 51: 2019 NYT Article 1948
Def't Exh. 53: Blumenthal-Markey Letter to FTC 1957

Gov't Exh. 1: CAST PowerPoint Presentation 1981
Gov't Exh. 2: Geofence Warrant (Doc. 54-1) ..... *see* J.A. 107
Gov't Exh. 3: Declaration of Marlo McGriff (Mar. 11, 2020)
(same as Def't Exh. 21 (Doc. 96-1)) ..... *see* J.A. 1551
Gov't Exh. 3a: Declaration of Sarah Rodriguez (Mar. 11, 2020)
(same as Def't Exh. 24 (Doc. 96-2)) ..... *see* J.A. 1579
Gov't Exh. 3b: Supplemental Declaration of McGriff (June 17, 2020)
(Doc. 110-1) 2032
Gov't Exh. 3c: Third Declaration of Marlo McGriff (Aug. 7, 2020)
(same as Def't Exh. 23 (Doc. 147)) ..... *see* J.A. 1562
Gov't Exh. 4: Joshua Hylton emails with Google 2034
Gov't Exh. 5: Google Privacy Policy 2048
Gov't Exh. 5a: Google Terms of Service 2081
Gov't Exh. 6: Special Agent D'Errico's C.V. 2088
Gov't Exh. 12: "Got to Be Mobile" Video ..... *see* J.A. 2091

VOLUME 9 (pages 2091 - 2092) – DIGITAL MEDIA EXHIBIT

Gov't Exh. 12: "Got to Be Mobile" Video (admitted only at suppression motion hearing) ..... (.mp4 file)

VOLUME 10 (pages 2093 - 2138) – SEALED DOCUMENT EXHIBIT

Def't Exh. 3: PDF of Raw Data (*see* Doc. 69 (sealing order)) (admitted at both discovery motion hearing and suppression motion hearing) 2093

VOLUME 11 (pages 2139 - end) – SEALED DIGITAL MEDIA EXHIBITS

Def't Exh. 5: Three Paths Video (admitted at both discovery motion hearing and suppression motion hearing) ..... (.mp4 file)
Def't Exh. 8: CSV Google Data File (admitted only at suppression motion hearing) ..... (.csv file, viewable in Excel)

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

MR. CHATRIE'S POST-HEARING BRIEF ON "GEOFENCE" GENERAL WARRANT

At the government's direction, Google searched the Location History ("LH") data of "numerous tens of millions" of people in an effort to generate suspects in the robbery. *See* Def. Ex. 21 at 4. It was a dragnet of epic proportions. The warrant seeks to dress up this search in a "three-step" process crafted by Google and the FBI, but that process is no more than a legal fig leaf obscuring the magnitude of the privacy invasion at work. This epic dragnet gave free reign to Google and the government to single out which accounts to search further in steps two and three. It was so overbroad and lacking in particularity that it was the digital equivalent of a general warrant and therefore impermissible under the Fourth Amendment. Mr. Chatrie seeks to suppress all evidence obtained as a result of the geofence warrant, and all fruits thereof.

BACKGROUND

In March 2021, this Court held an evidentiary hearing on Mr. Chatrie's motion to suppress the geofence warrant. *See* ECF 29. Mr. Chatrie had filed that suppression motion in October 2019, based on the sparse facts available to him at that time. What little defense counsel knew about geofence warrants came primarily from newspaper articles and online reports. *See id.* at 4-5. Over the past 18 months, however, investigation revealed significant new facts that have both merited corrections and strengthened Mr. Chatrie's legal arguments.

Specifically, Google filed an *amicus* brief (Def. Ex. 2), unsolicited, as well as four written declarations (Def. Ex. 21; ECF No. 96-2; ECF No. 110-1; Def. Ex. 23) in response to two defense subpoenas *duces tecum* (ECF No. 82; ECF No. 123). In addition, two Google representatives, Marlo McGriff and Sarah Rodriguez, testified in person over the course of two days. Tr. 190–275 282–424, 445–499.[1] The Commonwealth of Virginia provided some information about the qualifications of the magistrate judge who issued the warrant. *See* ECF No. 156. And defense counsel benefited from the expertise of Spencer McInvaille, who forensically examined Mr. Chatrie's phone, prepared two written reports (Def. Ex. 6; Def. Ex. 7), and testified twice in-person. *See* Tr. 16–170; 1/21/20 Tr. 17—139. Furthermore, counsel for Mr. Chatrie cross-examined the Virginia state investigator responsible for obtaining and executing the geofence warrant, Det. Joshua Hylton, Tr. 623–46, and FBI Special Agent Jeremy D'Errico, who offered expert testimony for the government. Tr. 550–93. Finally, three federal magistrates, all in the Northern District of Illinois, have issued opinions, *sua sponte*, regarding geofence warrants. *In re Search Warrant Application for Geofence Location Data Stored at Google* ("Harjani Opinion"), No. 20 M 525, 2020 WL 6343084 (N.D. Ill. Oct. 29, 2020); *In re Information Stored at Premises Controlled by Google* ("Fuentes Opinion"), 481 F. Supp. 3d 730 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google* ("Weisman Opinion"), No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020). Two of the three found the warrants invalid. *See* Fuentes Opinion, 481 F. Supp. 3d at 757; Weisman Opinion, 2020 WL 5491763 at *8. All three of them, however, did so without the benefit of adversarial briefing or the full factual record now before this Court.

Mr. Chatrie submitted a supplemental brief to the Court in May 2020. *See* ECF No. 104. Most significantly, by then, Google clarified that the geofence warrant required searching

[1] All cites to "Tr." refer to the March 4–5, 2021, hearing unless otherwise noted.

"numerous tens of millions" of people, not just the 19 who happened to be near to the bank. *See* Def. Ex. 21 at 4. Google subsequently confirmed this fact at the March hearing and provided additional context that supports Mr. Chatrie's argument in favor of suppression. Mr. Chatrie's arguments have evolved accordingly, and defense counsel has sought to keep the Court abreast of these developments. *See, e.g.,* ECF No. 104 at 2, 4; ECF No. 82 at 2–3. But in the interest of clarity, Mr. Chatrie summarizes the relevant facts as they are currently known.

FACTS

Someone robbed the Call Federal Credit Union in Richmond, Virginia, on May 20, 2019. *See* Def. Ex. 1 at 11. The Chesterfield County Police Department had no suspects. There were plenty of witnesses and surveillance videos, Tr. 607–08, but instead of pursuing traditional investigative techniques, the government turned to Google. Det. Joshua Hylton drafted an application for a "geofence" warrant, a novel digital search that required Google to identify all electronic devices in the area at the time of the robbery, and then provide even more data on devices of interest at the government's discretion. *See* Def. Ex. 1.

Det. Hylton had never received training on geofence warrants. Tr. 627–28. There was no training because there were no law enforcement procedures to follow. Tr. 552-53. In fact, neither the Chesterfield Police nor the FBI, who quickly became involved in this case, trained their investigators on seeking geofence warrants. *Id.*; Tr. 552. Agent D'Errico assisted in the investigation and testified as the government's expert on geofence warrants. Tr. 506–50. Yet, like Det. Hylton, Agent D'Errico admitted he has never received specific training on geofence warrants, from the FBI or from Google. Tr. 551.

This lack of training and absence of procedures does not mean that police conjured the geofence warrant here. The basic contours of a geofence warrant were the unofficial product of

repeated discussions between Google and the Computer Crimes and Intellectual Property Section ("CCIPS") of the Department of Justice in 2018.[2] Tr. 456-57. Google required a warrant because it considers Location History data to be "content" under the Stored Communications Act, 18 U.S.C. § 2703, which requires a warrant to access it. *See* Def. Ex. 2 at 16.[3]

Eventually, Agent D'Errico obtained a "go by" from CCIPS, which "assists" investigators "in the language needed to obtain a geofence search warrant" from Google. Tr. 552; *id.* at 553 ("[W]e follow the steps that [CCIPS and Google] have laid out in order to … make sure that Google understands what we are requesting and that we understand what we'll receive back"). Agent D'Errico does not recall providing this "go by" to Det. Hylton, at least in this case. Tr. 553. But somehow or another—he does not recall—Det. Hylton got one too. Tr. 635. In fact, Det. Hylton had sought a state geofence warrant once before using a local "go by" from another officer, so he used the same template, plugged in the new date and location, and did it again. Tr. 631.

I. Location History

The warrant outlined a three-step process for Google to search users' location data and provide information about nearby devices around the time of the robbery. The warrant did not instruct Google to exclude any types of location data from the search. Rather, it called for searching "each type of Google account," regardless of the device configuration. Def. Ex. 1 at 4, 9. Instead, Google searched one of its three databases: the so-called "Sensorvault" database, which is the repository for "Location History" data. *See* Tr. 211-12; ECF No. 104 at 6-7.

[2] Tr. 456-57 ("CCIPS is an agency that … our counsel engages with to discuss sort of certain procedures that may be relevant for the way that … Google will need to handle these types of requests, especially with reverse Location History being a relatively new type of request"); 476 (repeated "engagement" between CCIPS and Google "help[ed] to socialize the concept of these types of warrants"); *see also* Tr. 552-53 (discussing the relationship with CCIPS).

[3] The government disputes Google's characterization of Location History data as user "content," *see* ECF No. 109 at 9; ECF No. 71 at 8, but it has yet to cite to a single case where a subpoena or court order have been sufficient to obtain Location History data.

Location History is a Google feature that logs device location data and creates a timeline on a map of where a user has been with that device. Def. Ex. 21 at 2; Tr. 355. Google likens Location History data to a virtual "journal" of where users have been (with their devices). Def. Ex. 2 at 6; Tr. 204. When Google saves this data, it associates it with unique user accounts it keeps in the "Sensorvault." Def. Ex. 21 at 3; Tr. 130, 314. If a user has the Google Location History enabled, then Google estimates the user's device location using Global Positioning System ("GPS") data, the signal strength of nearby Wi-Fi networks, Bluetooth beacons, cell phone location information ("CSLI") from nearby cellular towers, and Internet Protocol ("IP") address information. Tr. 18–19; Def. Ex. 21 at 4, 8–9. Location History is not an "app"; it is a setting on the Google account associated with a device. Once enabled, it records that device's location as often as every two minutes, at all times regardless of whether any app is open or closed, the phone is in use, or the device is in a public or private space. Tr. 20, 114-15, 436–37, 513. Approximately one-third of all active Google users have Location History enabled on their accounts. Def. Ex. 21 at 4; Tr. 205. Google has been unable or unwilling to say exactly how many users this was in 2019, but Google acknowledges that it was at least "numerous tens of millions" of people. *Id*.

II. Location History Accuracy

The accuracy of Location History information varies depending on which sources of location data are available to the device at a given time. For example, location data based on GPS signals is usually more accurate than location derived from Wi-Fi signals. *See* 1/21/20 Tr. at 64. Google, however, has a preference. Google relies on Wi-Fi signals first, followed by GPS, then Bluetooth, and finally CSLI. Even though GPS data is generally more accurate than Wi-Fi, GPS consumes more resources on the device, diminishing battery life and making it impractical to use frequently. Tr. 519. As a result, Location History data often comes from Wi-Fi data, and that is what happened

in this case. Here, 88% of the coordinates at issue were derived from Wi-Fi signals; the remainder came from GPS. *See* 1/21/20 Tr. at 64. None were derived from Bluetooth, CSLI, or IP address information. *Id.*; *see also* Tr. 173.

Location History data is Google's ***estimation*** of where a device is. Tr. 212. It is not hard data, but is instead Google's best guess at device location based on available information. *See* Def. Ex. 2 at 10–11 n.7 ("In that respect, LH differs from CSLI, which is not an estimate at all, but simply a historical fact: that a device connected to a given cell tower during a given time period. An LH user's Timeline, however, combines and contextualizes numerous individual location data points …"). As Google puts it, Location History is a "probabilistic estimate," and each data point has its own "margin of error." *Id.* Google uses an unknown algorithm to make this estimation, which Google did not disclose when subpoenaed. *See* ECF No. 82 at 10; ECF No. 85 at 2. Indeed, Location History is different from other types of location data that courts have previously considered and emerges from Google's black box with a fluctuating margin of errors. *See* Tr. 178, 590–91.

When Google reports a set of estimated latitude/longitude coordinates, it also reports a "confidence interval," or "Map Display Radius," to indicate Google's confidence in its estimation. Tr. 38, 212, 530–31. On a map, Google visualizes the coordinates as a "blue dot" and the Display Radius as a "shaded circle" around the dot. *See* Tr. 213; Def. Ex. 21 at 9. The government illustrates this concept (in red) in a report Agent D'Errico prepared, as shown in Figure 1. *See* Gov't Ex. 1 at 18.

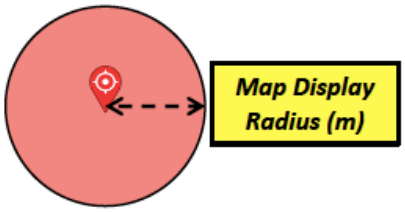
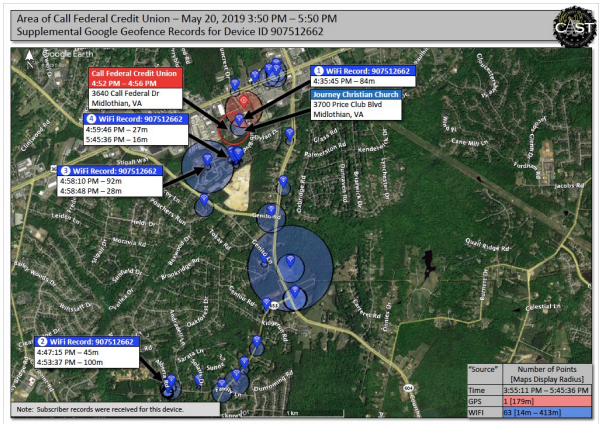


Figure 1

Importantly, Google is equally confident that a device could be anywhere within the Display Radius, *i.e.*, the shaded circle. *See* Tr. 214. The estimated coordinates, recorded as

latitude/longitude, are simply the center point of that circle. *See* Tr. 531 ("If I could, I would draw maps without a center point in it and just a bubble because that's a better representation."). It is equally likely that the device is at the center point as anywhere else in the shaded circle, even off toward the edge. *See* Google, *Find and Improve your Location's Accuracy* (last visited Apr. 26, 2021) ("The blue dot shows you where you are on the map. When Google Maps isn't sure about your location, you'll see a light blue circle around the blue dot. You might be anywhere within the light blue circle.").[4] Indeed, Google users may be familiar with this phenomenon, as "in the common scenario of realizing that your cell phone GPS position is off by a few feet, often resulting in your Uber driver pulling up slightly away from you or your car location appearing in a lake, rather than on the road by the lake." *Harjani Opinion*, 2020 WL 6343084 at *9.

The Map Display Radius expands and contracts in accordance with Google's confidence in its location estimation. As a result, the accuracy of Location History data varies over time, as illustrated by the varying size of the shaded circles in the government's rendition of user data in this case, as shown in Figure 2 below. ***Figure 2***



Google always aims to be 68% confident that a device is somewhere within the Display Radius. Tr. 39; *see also* Tr. 581 ("68% is approximately the industry standard"). In other words,

[4] *Available at* https://support.google.com/maps/answer/2839911?co=GENIE.Platform%3DAndroid&hl=en.

Google simply changes the size of the Display Radius, or shaded circle, in order to achieve 68% confidence. As Google explains, "The smaller the circle, the more certain the app is about your location." Google, *Find and Improve your Location's Accuracy* at 1. By contrast, a large circle means that Google is less confident in a user's location, indicating that they could be anywhere within a much larger area, the product of a larger Display Radius. *See* Tr. 213, 530-31. There is always a 32% chance a device is outside of the Display Radius altogether. *See* Tr. 213. Or in other words, the odds are better than 1-in-4 that the user's actual location lies beyond the shaded circle.

III. Location History Advertising

Google appears well satisfied with the 68% accuracy industry standard. *See* Tr. 581. According to Google, "the resulting picture of the user's location and movements is sufficiently precise and reliable for the purposes for which it was designed." Def. Ex. 2 at 10 n.7. For Google, Location History has two purposes: (1) to support a "Timeline" map for users, *see* Tr. 195, and (2) to provide targeted advertising based on a user's location, *see* Tr. 22-23, 196–98, 301. Neither function, however, relies on a high degree of accuracy for any data point. Rather, Google infers a user's Timeline from a series of data points even when an "outlier" strays from the logical path. *See* Tr. 195–96. For advertising purposes, Google actively obscures individual device information, preventing businesses from being able to track particular users. *See* Tr. 197.

Google uses Location History for a specific advertising purpose—to calculate "store visit conversions." A "store visit conversion" refers to a user who saw a Google-placed advertisement and then visited the relevant business in person. Tr. 196–97. Location History is not used for other types of location-based advertising, such as "radius targeting," Tr. 197–98, which allows businesses to show an ad to all devices in a given area. As Google explains, "Location History does not power all ads. … [A]ny geotargeting or other use of Location for ads is coming from the

location services at the device level." Tr. 367–68. So, although businesses can use Google to target advertising based on a device's location, they cannot do sousing Location History. Tr. 198.

Regardless of the advertising type, however, Google "never share[s] anyone's location history with a third party." *See* Tr. 197. Google is "not giving user location data over to stores about who was around." Tr. 197. Even when Google uses location data sources other than Location History, such as "Web & App Activity," the smallest possible radius available to advertisers is a kilometer. Tr. 198. This is done for privacy purposes, so that those advertisers do not actually get to see which devices were in the area. Tr. 197, 199. Likewise, advertisers cannot go back to Google and ask for more information about where certain devices were before or after they saw an ad or visited a store. Tr. 199. Advertisers simply cannot get any identifiable information about individual Google users. Tr. 199; *see also* Tr. 23 (explaining that the data in warrant returns is "much different" than what is accessible to advertisers).

IV. Enabling Location History

Google asserts that Location History is an "opt-in" feature for Google users, Def. Ex. 1 at 12, which means that a user must actively enable it at some point in order for it to work. There are, however, many different ways for a user to enable Location History, either through the device settings or through certain Google applications. Def. Ex. 6 at 4; Tr. 74; *see* Tr. 285–86.

One possibility is to enable Location History during the initial setup of a new device. As demonstrated by defense expert Spencer McInvaille during the January 2020 discovery hearing, Google first prompts users to enable Location History during the initial phone setup process. *See* 1/21/20 Tr. at 51. If a user does not opt-in at that point, Google will prompt them to enable Location History through pop-up screens, known as a "consent flow," when opening certain Google applications or using certain Google features.

Another way to enable Location History is to set up Google applications that rely on location information. These apps include the primary Google App (for search queries), as well as Google Maps, Google Photos, and Google Assistant. *See* Tr. 221, 285–86. If a user does not enable Location History while setting up the device, Google prompts them to do so before they can use any of these applications. *See* Tr. 350–52. For example, as the defense demonstrated through video evidence and detailed expert testimony, Google prompts users to enable Location History when first opening Google Maps following the setup of a new phone. 1/21/20 Tr. at 55–56. The whole process took under five minutes and did not mention Location History by name. *Id.* at 56–57.

In this case, a combination of Google data and an extensive forensic analysis of Mr. Chatrie's phone revealed that Location History was likely enabled through the Google Assistant setup process, shortly after midnight on July 9, 2018. Def. Ex. 6 at 4–5; Tr. 76–77, 286–87. Two basic facts led to this conclusion. *See* Def. Ex. 6 at 4–5. First, Google reported that Location History was enabled on Mr. Chatrie's account on July 9, 2018, at approximately 4:09 Universal Time Code ("UTC"), or 12:09 a.m. Eastern time. *See* Def. Ex. 6 at 2; Def. Ex. 23 at 2. Second, Mr. Chatrie's phone shows that Google Assistant was installed two minutes earlier, at 4:06:51 UTC. A Google "Audit Log" shows three timestamps indicating changes to the Location History setting occurred just seconds later at 04:07:25 UTC, 4:09:08 UTC, and 04:09:08 UTC. *See* Def. Ex. 6 at 4. Therefore, Mr. McInvaille concluded that "it is likely Google Location History was enabled using the Google Assistant application." Def. Ex. 6 at 5. Neither the government nor Google can challenge this conclusion. *See* Tr. 287.

When a user who does not have Location History enabled attempts to use Google Assistant for the first time, Google displays a pop-up box that is part of a "consent flow" that prompts the user to enable up to three Google features, including Location History. This pop-up box will also

appear if the user "long press[es] the home button" on an Android device that does not have Google Assistant set up. Tr. 79; Tr. 351. A "long press" means leaving one's finger on the button for a moment, as opposed to tapping it quickly; the "home button" is the big button at the bottom of the screen. On Android devices like Mr. Chatrie's, a long press of the home button will activate Google Assistant, as if a user had opened the application by tapping on an icon.

Neither Google nor any party has been able to definitively state how this "consent flow" would have appeared on Mr. Chatrie's device on July 8, 2018. Tr. 81, 298. There are two possibilities, however. *See* Def. Ex. 7 at 1–3; Tr. 298. First, the screen could have read: "Creates a private map of where you go with your signed-in devices" with a blue "YES I'M IN" button, as shown below in Figure 3. *See* Def. Ex. 7 at 2. Alternatively, the screen could have read: "Saves where you go with your devices" with a blue "TURN ON" button, as shown below in Figure 4. *See* Def. Ex. 7 at 4; Def. Ex. 23 at 8; Tr. 102, 298. Google calls this line the "descriptive text." Tr. 328. Above both versions of the descriptive text, at the top of the screen, was a sentence that read: "The Assistant depends on these settings in order to work correctly." Def. Ex. 7 at 3. And at the bottom of the screen, separated by a line and in lighter and less-contrasting font, were two additional sentences indicating that this data "may be saved" and that "You can see your data, delete it and change your settings at account.google.com." Def. Ex. 7 at 4; Def. Ex. 23 at 8.

Figure 3

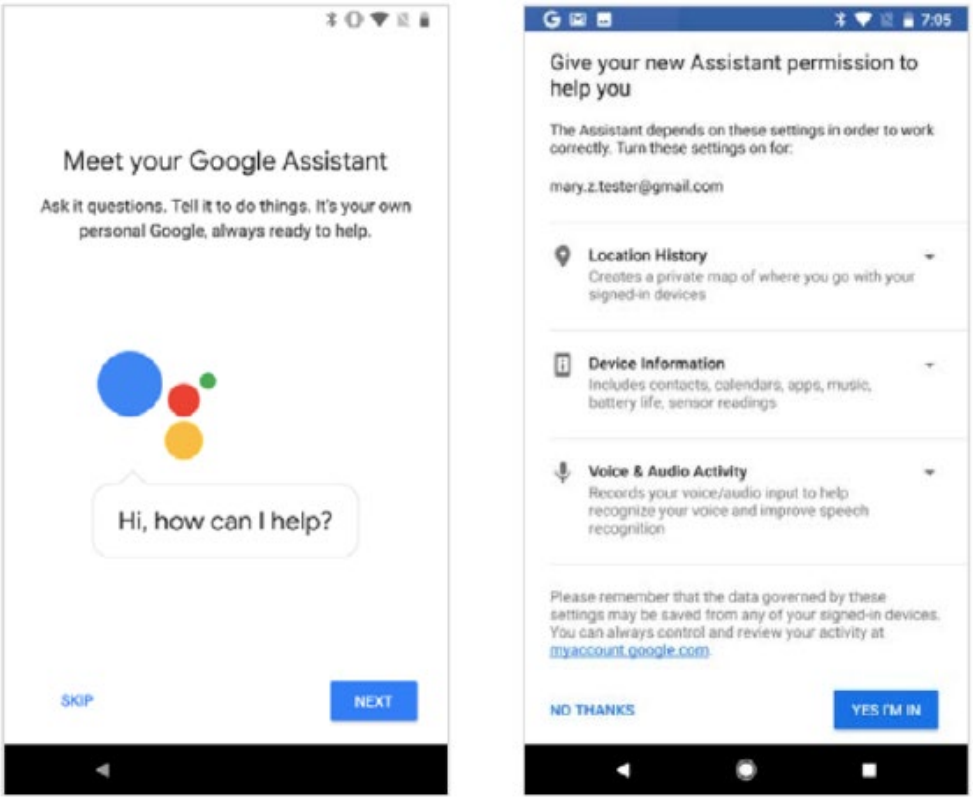


Figure 4

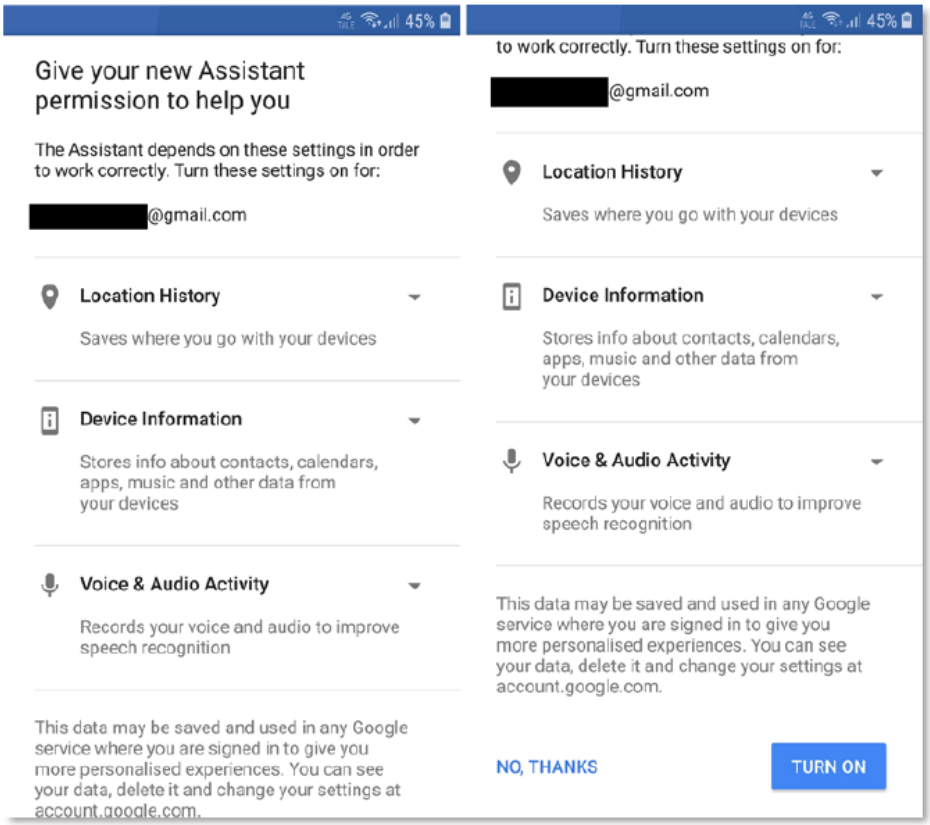
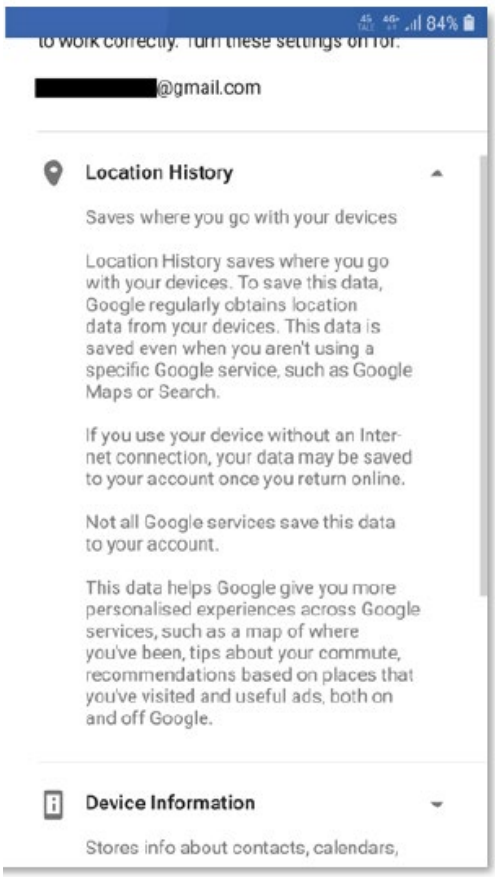


Figure 5



As shown here in Figures 3 and 4, this screen would have asked users to enable two other Google settings—"Device Information" and "Voice & Audio Activity"—if not already enabled. Def. Ex. 7 at 3; Tr. 109, 333. If presented with more than one permission, a user would have had to enable all of them together, or else quit the Google Assistant setup. Tr. 109, 334. In other words, users were not given the option to make an individual determination with respect to each of the three possible permissions. *Id.*

Additional information, which Google calls the "consent copy text," is shown only if users tap on the "expansion arrow," the small triangle on the other side of the page from "Location History." *See* Tr. 106, 329. Figure 5 depicts this "copy text" for Location History, which would have been the same regardless of which "descriptive text" appeared. *See* Def. Ex. 7 at 3; Tr. 271. **Users are not required to view the "copy text."** Tr. 330. Only users who tap the expansion arrow will see it. Def. Ex. 7 at 3; Tr. 110, 345. **And users can enable Location History without ever seeing this information.** *See* Tr. 110, 330, 335.

The Google Assistant setup screen did not contain or link to Google's Privacy Policy. *See* Def. Ex. 7 at 1–4. Users who nonetheless viewed Google's Privacy Policy during the relevant timeframe—from when Mr. Chatrie enabled Location History in July 2018 to his arrest in September 2019—would have seen two different versions of the policy depending on when they accessed it. In the first iteration, in effect from May 2018 to January 2019, the Privacy Policy

mentioned "Location History" twice. *See* Tr. 294. The first reference read: "You can also turn on Location History if you want to save and manage location information in your account." Def. Ex. 43 at 7. The second reference stated: "Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions." *Id.* at 8. The next iteration of the Privacy Policy covered January 2019 to October 2019, and changed the first reference to read: "You can also turn on Location History if you want to create a private map of where you go with your signed-in devices." Def. Ex. 44 at 7. The second reference remained the same. *See id.* at 8.

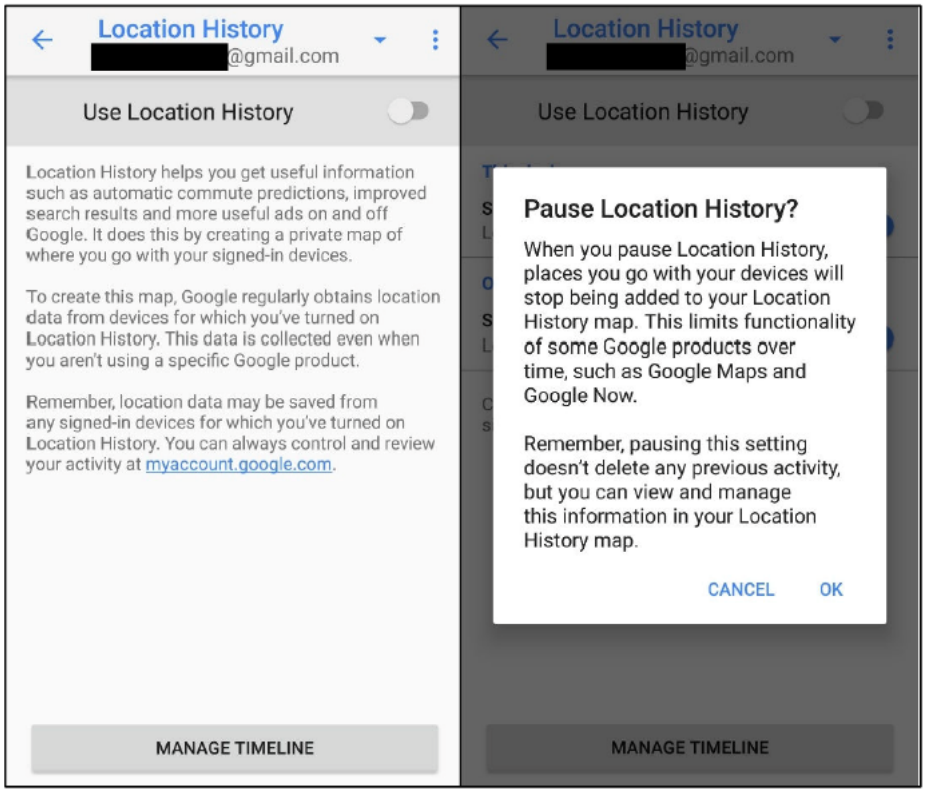
V. "Pausing" Location History

Once enabled, Location History cannot be turned "off," only paused. Tr. 360–61. There are three ways to pause Location History: (1) in the settings for an application like Google Assistant, (2) in the settings panel for the device, or (3) by logging in to "myactivity.google.com" and changing the account's settings. *See* Tr. 340–41. These are the only methods of pausing Location History. **If a user disables or stops using Google Assistant, for example, Location History is still enabled and running**. Tr. 123-24, 362. A user has to know to actively navigate one of these paths in order to locate and pause Location History. Tr. 341. Upon doing so, Google would display another pop-up screen containing text called the "pause copy," as shown in Figure 6. Def. Ex. 27 at 23.

The text of the "pause copy" warns users that pausing Location History will "limit[] functionality of some Google products over time, such as Google Maps and Google Now." It does not specifically mention Google Assistant or provide any details about how app functionality might be limited. In fact, Google Assistant will continue to function with Location History paused, but

Google does not inform users of this option, either when setting up the application or when displaying the "pause copy." *See* Tr. 339, 343.

Figure 6



VI. Deleting Location History

Just as pausing Location History does not delete Location History data, disabling Google Assistant does not delete Location History data. That requires manual input. *See* Tr. 356, 361. Google now offers an "auto-delete" function that allows users to automatically delete Location History data older than three months, *see* Def. Ex. 46, but this function was unavailable for Mr. Chatrie. Tr. 356. To delete Location History data manually, a user must access the "Timeline UI," or user interface, at which point records can be deleted by day or date range. Tr. 356. Deleting Location History records will not stop Location History from continuing to collect data. Tr. 188.

VII. The Geofence Warrant

The warrant in this case authorized the search of all Google Location History data, for all users, in order to identify devices of interest and obtain additional information about those accounts. The warrant outlines a dependent, three-step process, now familiar to this Court. *See* Def. Ex. 2 at 12–14; *see also* ECF No. 29 at 4–7; ECF No. 104 at 1–2.

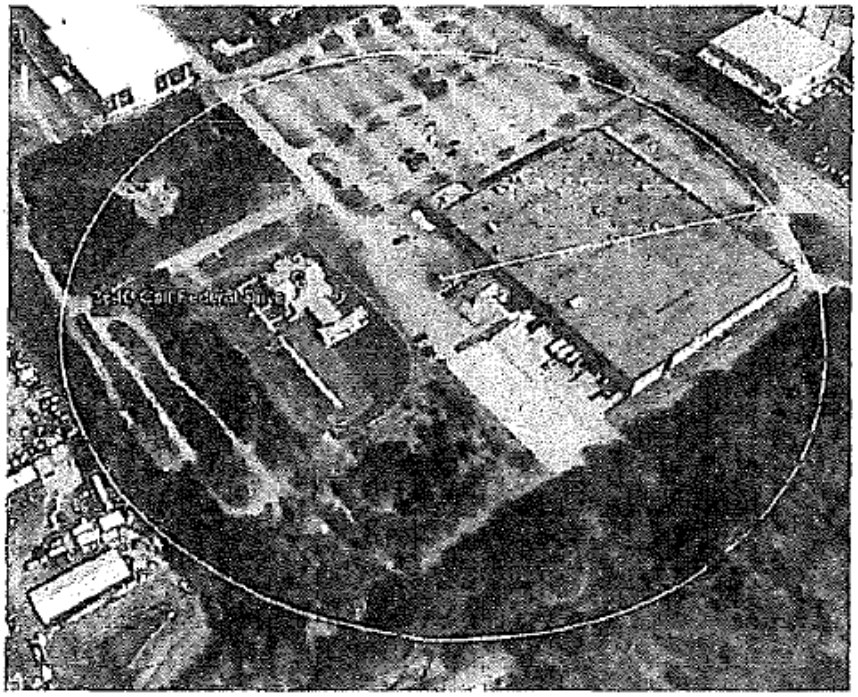
Step one required Google to search the Sensorvault to determine which devices were purportedly within 150 meters of the Call Federal Credit Union during the time of the robbery as well as 30 minutes before and after it occurred. Def. Ex. 1 at 4. To carry out this command, Google had to search the contents of every account with Location History enabled, *i.e.*, "numerous tens of millions" users, for records satisfying the government's criteria. Tr. 29, 52–53, 204–05. It is impossible to search only users who were within 150 meters of the bank because there is "no way to know ex ante which users may have [Location History] data indicating their potential presence in particular areas at particular times." Def. Ex. 2 at 12. Rather, "Google must search across all Location History journal entries to identify users with potentially responsive Location History data, then run a computation against every set of coordinates to determine which Location History records match the time and space parameters in the warrant." Tr. 204 (quoting Def. Ex. 2 at 12).

Google ultimately identified 19 accounts with responsive data. The government seized those records in a database file containing 210 location points on June 28, 2019. Tr. 132, 642. Google states it provided this data in "anonymized" form, meaning that it did not include account names or usernames. Tr. 404. It did, however, contain a "Device ID" number, a unique number in Sensorvault linked to the user's device that does not change over time. Tr. 451, 453–54.

Google identified this data by selecting any devices with an estimated latitude/longitude inside the 150-meter geofence from the warrant, shown in Figure 7. For some of these location

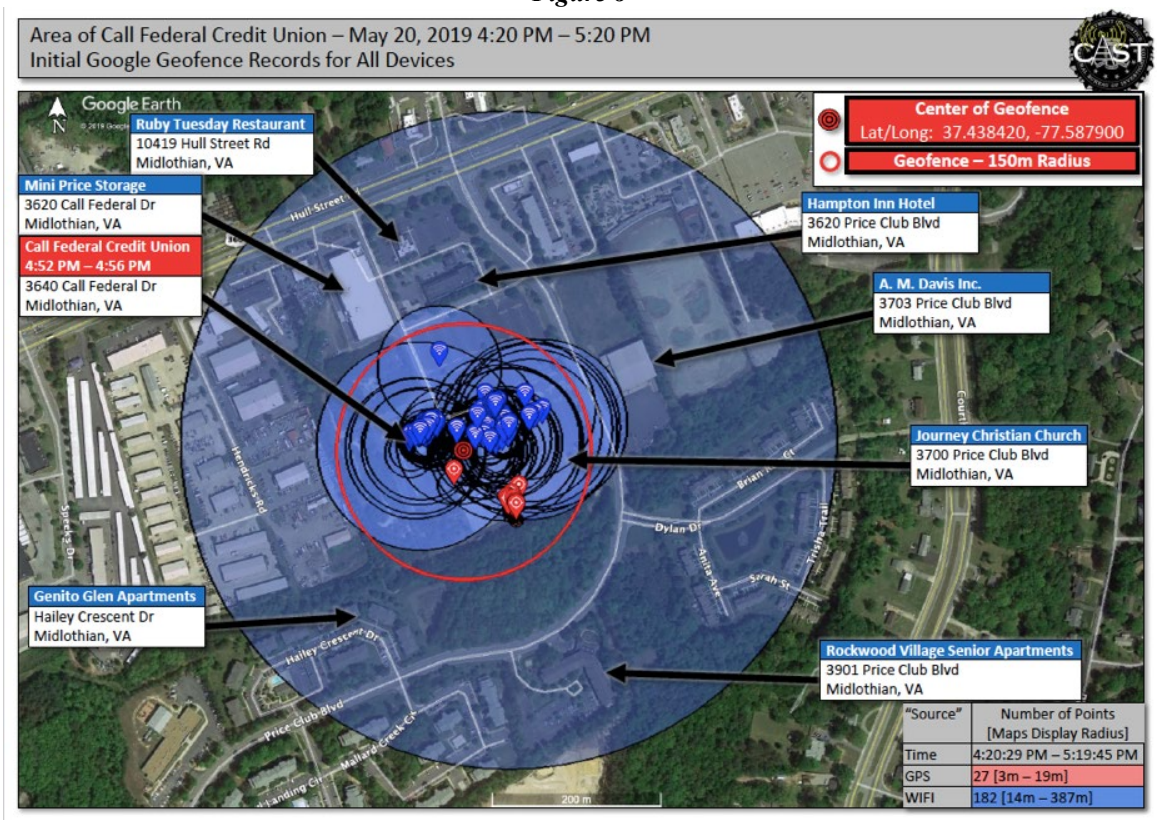
points, however, the Map Display Radius extended beyond the geofence, meaning that the device was just as likely to be outside the boundary. *See supra* at 7; Tr. 587–88. Both Google and the government acknowledge this possibility of "false positives." *See* Tr. 586; Def. Ex. 2 at 9, 20 n.12.

Figure 7



The largest Display Radius is 387 meters from coordinates near the center of the 150-meter geofence. *See* Def. Ex. 3 at 6–12, 17–37. Consequently, the effective range of the search was more than twice as far as the geofence requested in the warrant. Tr. 41–42. Agent D'Errico notes that the actual location of that device remains unknown, meaning that it could have been inside or outside the geofence. *See* Tr. 587. All agree, however, that there is a 68% chance it was somewhere in the largest blue circle depicted in Figure 8 below. Tr. 39–40, 215, 587. That circle encompasses not just the bank and the Journey Christian Church, but also multiple streets plus all of the businesses and residences nearby—including Hull Street and Price Club Drive, Ruby Tuesday's, the Hampton Inn, A.M. Davis, Inc., Mini Price Storage, the Genito Glen Apartments, and the Rockwood Village Senior Apartments. *See* Tr. 32–33, 49; 1/21/20 Tr. at 66–67.

Figure 8



Step two of the warrant process required the government to review the step one data and "attempt to narrow" the list of devices. Def. Ex. 1; Tr. 592. Google would then provide two hours of additional Location History data for a subset of those devices, called "contextual" data, for one hour before and after the robbery. *Id.*; Tr. 26, 30.

Initially, Det. Hylton sent two emails on July 1 and 2, 2019, each requesting contextual data for all 19 devices from step one. *See* Gov't Ex. 4; Tr. 472, 622; ECF No. 96-2 at 5. Det. Hylton also requested the subscriber information for all 19, *i.e.*, "de-anonymized" records that the warrant reserved for step three. *Id*. Det. Hylton sent these emails after consulting with the United States Attorney's Office. Tr. 622. When Det. Hylton did not receive a reply from Google, he left two voicemails on July 8, 2019. Tr. 621–22, 642. A Google specialist called back the same day and specifically advised Det. Hylton that the warrant required the government to narrow the number of devices for which they were seeking expanded data. Tr. 473–74. Google did not say by how

much the government had to narrow the list, but advised it was required. *Id.* at 474. The Google specialist also had to advise Det. Hylton about what types of information would be produced in the later stages of warrant. *Id.* The specialist reported to her supervisor, Ms. Rodriguez, that it did not appear Det. Hylton was familiar with the process outlined in the warrant. Def. Ex. 24 at 5-6.

Following the July 8 phone conversation with Google, Det. Hylton emailed Google once again, this time requesting stage two data (only) for nine of the 19 devices. Tr. 642. Accordingly, Google created another database file on July 9, 2019, containing the "contextual" data for those nine devices and sent it to the government. *See* Def. Ex. 8.

Step three of the warrant required the government to further cull the number of devices and identify an even narrower subset. Tr. 26, 543–44; Def. Ex. 1. Google would then produce de-anonymized account information, including the username and subscriber information, associated email addresses and telephone numbers. *Id*. The government twice requested this data for three devices on July 10 and 11, 2019. Tr. 643. On July 11, Google sent the government a third database file matching each "Device ID" with its "Gaia ID" as well as records reflecting the associated subscriber information. Tr. 544. One of those three subscribers was Mr. Chatrie.

ARGUMENT

The geofence warrant was an unconstitutional search that intruded upon Mr. Chatrie's reasonable expectation of privacy in his Google data. For the reasons set forth below, Mr. Chatrie maintains that the warrant was invalid because it was a general warrant, fatally overbroad and devoid of particularity, and therefore impermissible under the Fourth Amendment. *See* ECF No. 29 at 7, 16–24; ECF No. 104 at 10. The *Leon* good faith doctrine does not apply because the warrant was so obviously deficient that it was *void ab initio*. As a result, this Court should suppress the results of the geofence warrant, including all of the fruits thereof.

I. Mr. Chatrie Had a Reasonable Expectation of Privacy in His Location History Data.

Mr. Chatrie enjoys a reasonable expectation of privacy in his Location History data following the Supreme Court's landmark decisions in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *United States v. Jones*, 565 U.S. 400 (2012). Although the shortest search at issue in either case involved seven days of cell phone location information for a single individual, *see Carpenter*, 138 S. Ct. at 2217, the Court's reasoning applies with at least equal force here. *See* ECF No. 104 at 10; ECF No. 29 at 9.

A. Location History Is At Least As Precise as CSLI

Location History data is at least as precise as the CSLI in *Carpenter*. *See* ECF No. 104 at 12–14. The government concedes this point. *See* ECF No. 41 at 8; ECF No. 109 at 9. In this case, all of the estimated Location History points derive from either Wi-Fi or GPS signals, which Google states are "capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI." Def. Ex. 21 at 4. Additionally, 12% of the data points in this case are from the same type of GPS signals at issue in *Jones*, which can be accurate to less than a meter. *See* Tr. 18–20; ECF No. 29 at 8; ECF No. 104 at 14.

But, Google did not design Location History to solve bank robberies. Google's estimation of a device's location may be "sufficiently precise and reliable for the purposes for which it was designed," *i.e.*, creating a user Timeline and targeting advertisements within a kilometer. Def. Ex. 2 at 10 n.7.; *see also supra* at 8. But because Google did not design Location History to respond to 150-meter geofence warrants, its ability to accurately do so comes with caveats, such as the possibility of "false positives," *see supra* at 8, 17, and "false negatives." *See* Tr. 44–45, 47–48, 217, 585. Also, due to the Map Display Radius, the effective range of the search extended more than twice as far as the 150-meter circle described in the geofence warrant. *See supra* at 17.

B. A Search of Location History Data Is Highly Intrusive

A search of even small amounts Location History data is highly intrusive. As the government recognizes, *Carpenter* "explicitly declined to determine whether there is a 'limited period' for which the government can acquire cell phone location information without implicating the Fourth Amendment." ECF No. 41 at 7. Short-term searches are capable of revealing the "privacies of life," 138 S. Ct. 2214, which was the Court's main concern in both *Carpenter* and *Jones*.

Although *Jones* and *Carpenter* involved so-called "long-term" searches,[5] what motivated the Court in each instance was the risk of exposing information "the indisputably private nature of which takes little imagination to conjure: 'the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.'" *Jones,* 565 U.S. at 415 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 441–42 (2009)); *accord Carpenter*, 138 S. Ct. at 2215. Thus, "[i]n cases involving even short-term monitoring, some unique attributes of GPS surveillance … will require particular attention." *Jones*, 565 U.S. at 415. The same is true for cell phone location information, given that "[a] cell phone faithfully follows its owner beyond public throughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter*, 138 S. Ct. at 2218.

Even before *Jones* and *Carpenter*, the Supreme Court was concerned with short-term location tracking, especially when it reveals information about the interior of a constitutionally-protected space, such as a home. In *United States v. Karo*, the Court found that using an electronic beeper to track an object inside a private residence was a search. 468 U.S. 705, 716 (1984). A

[5] In fact, the government's demand for seven days of data in *Carpenter* netted only two days of data. *See* 138 S. Ct. at 2212.

search occurs at the moment the object "has been withdrawn from public view." *Id.* at 717. Especially relevant here, the Court remarked that "[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight." *Id.* at 716. So too in *Kyllo v. United States*, the Court found that using a thermal imaging device to peer through the walls of a private residence was a search. 533 U.S. 27, 37 (2001). It was a search despite the fact that the scan "took only a few minutes" and could not show people or activity inside. *Id.* at 30. As the Court explained, "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained." *Id.* at 37.

Here, the geofence search revealed Google users inside the bank as well as in nearby homes, apartment complexes, a hospital, and the Journey Christian Church. *See* 1/21/20 Tr. at 80–90 (describing the paths for "Mr. Green," "Mr. Blue," and "Ms. Yellow"). Although Google had "anonymized" this data, the defense was easily able to determine the likely identities of at least three individuals. *See* Tr. 62–70; ECF No. 104 at 12; 1/21/20 Tr. at 83, 87–88, 90–91. This is why Google treats Location History data not as a "business record" but as sensitive user "content" under the Stored Communications Act, 18 U.S.C. § 2703, likening it to a "digital journal" of users' movements and travels and requiring a warrant to search it, even for two hours of data. *See* ECF No. 104 at 12; Def. Ex. 2 at 16. Furthermore, once the government seizes the "anonymized" Device IDs in steps one and two, it could simply obtain the subscriber information for any Device ID by issuing a subpoena to Google. In Illinois, Judge Fuentes recently denied a geofence warrant application in which the government promised to forego step three, finding that there is "no practical difference between a warrant that harnesses the technology of the geofence, easily and cheaply, to generate a list of device IDs that the government may easily use to learn the subscriber

identities, and a warrant granting the government unbridled discretion to compel Google to disclose some or all of those identities." *See* Fuentes Opinion, 481 F. Supp. 3d at 754.

Focusing only on the length of the search, however, is to ignore the unprecedented breadth of a geofence warrant, setting it apart from the individualized searches in *Jones* and *Carpenter* (and most every other case). This was not a search of one person's data over the course of one or two hours; it was a search of "numerous tens of millions" of people, all at once.

The government argues that this defining feature of a geofence warrant is irrelevant to the Fourth Amendment analysis, *see* ECF No. 109 at 8. But as Justice Gorsuch remarked, "On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not?" *Id.* at 2267 (Gorsuch, J., dissenting). The fact that the government is searching millions multiples the privacy intrusion.

C. Mr. Chatrie Did Not "Voluntarily" Share Location History Data With Google

The government contends that Mr. Chatrie has no expectation of privacy in his Location History records because Location History is an "opt-in" service and he "voluntarily" shared this data with Google. *See* ECF No. 109 at 5; ECF No. 41 at 10–12. But Mr. Chatrie maintains that, as in *Carpenter*, the question is not whether there was an agreement between an individual and a service provider. The question is whether, in a "meaningful sense," users "voluntarily 'assume[] the risk' of turning over a comprehensive dossier of [their] physical movements" to the government. *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745). But based on the facts in this case, it is clear that typical users like Mr. Chatrie would have no idea what Location History is, how it works, or whether they have it enabled on their phones.

An examination of the "opt-in" process reveals that the act of enabling Location History could not have been meaningful or informed, but was perfunctory at best and deceptive at worst.

This is evident on its face from the evidence presented to this Court about how the "consent flow" pop-up screen appears in Google Assistant. *See supra* at 11–13. It is also bolstered by the highly public and highly negative "feedback" that Google received regarding Location History and consent, reflected in changes that Google made to Location History after the facts of this case. And it is further demonstrated by the words of Google's own engineers, who repeatedly emailed a massive, company-wide discussion group to express their frustration over Google's lack of clarity with respect to location tracking permissions, and with Location History specifically.

First, consider the "opt-in" process. Google describes it as a complex seven-step process. Def. Ex. 2 at 7–8; Def. Ex. 21 at 2–3. But for Mr. Chatrie, it boiled down to a single pop-up screen in Google Assistant, at midnight, a week after he got the phone. *See supra* at 10.[6] That screen had one phrase of "descriptive text" about Location History. It in no way indicated that location data would be saved by Google, as opposed to stored locally on the device. It did not begin to convey the fact that it would operate independently of Google Assistant or convey that Google would collect location data constantly, at an average of every two minutes. *See supra* at 5. While additional information was available, users would have had to actively seek it out. Even then, what little else Google said about Location History did not adequately convey how it functioned.

There is a vast chasm between the reality of Google's Location History data collection and the advisements it actually requires users to read. To begin with, the "descriptive text" for Location History—the only text a user is actually required to read—is not only inadequate but outright confusing. One iteration tells users that it "Creates a private map of where you go with your signed in devices." *See supra* at 11. A later version says that Location History "Saves where you go with

[6] Previously, counsel for Mr. Chatrie suspected that the opt-in to Location History occurred either during the initial setup of the device, or upon opening an application like Google Maps. *See* ECF No. 104 at 15–18; Def. Ex. 21 at 2–3; Def. Ex. 2 at 12.

your devices." *See id*. In either event, a user might reasonably infer that this "private map" or saved data would be saved only on their device, not with Google. Tr. 301, 346 (descriptive text does not make a "distinction" as to whether location information is saved on-device or on Google servers).[7] In fact, that is how certain personalized features work on Apple Maps, available on Apple iPhones. *See Privacy*, Apple, https://www.apple.com/privacy/features/ (last visited Apr. 23, 2021) (describing how certain personalized features on Apple Maps "are created using data on your device" to "help[] minimize the amount of data sent to Apple servers"). Unless a user actively clicked the small "expansion arrow" on the other side of the screen from "Location History," there would be no indication that the data is saved in the cloud on Google's servers. *See supra* at 13; Tr. 110, 330. Google does not maintain records on who or how many people click the expansion arrow, Tr. 365, and there is no indication that Mr. Chatrie did here.

Additional language appeared at the bottom of the screen, away from the Location History "descriptive text," and in lighter font. There are two potential versions of this language, *see supra* at 11-12, but both state that this "data may be saved" and that "You can see your data, delete it and change your settings at account.google.com." *Id*. Neither version mentions Location History or location data, nor gives any indication of what it is, let alone that the phone will begin to transmit its location to Google every two minutes in perpetuity. It does not mention the Location History "Timeline," the virtual "journal" that is supposedly the reason users enable Location History.

Google did not require users to view any other text before enabling Location History, Tr. 110, 330, and, the other optional information it provided did not put users on notice about the true nature of the Sensorvault database. The expanded "consent copy," for instance—viewable only if a user clicked on the expansion arrow near "Location History"—explained that Google would

[7] Mr. McGriff testified that Google does not ascribe any significant difference in meaning between these two variations, s*ee* Tr. 301, raising the question of why the change occurred at all. *See infra* at 35.

obtain location data from users' devices, but it contained no warning about the frequency or sheer quantity of data collected. Tr. 347–48; *see* Def. Ex. 7 at 3. In this case alone, the Location History records revealed that Google collected location information every six minutes, twenty-four hours a day, seven days a week. Tr. 122, 436. On average, Google collects Location History data as often as every two minutes. *See supra* at 5. Nothing in the "descriptive text" or the "consent copy" explains the volume of information that Google plans to collect.

Additionally, nothing explains that Location History will operate independently, regardless of whether the phone is in use. The government contends that Mr. Chatrie's "voluntary disclosure of location information to Google is evident from the nature of the location-based services (like mapping) that Google provided him." ECF No. 109 at 9–10. But this argument falls flat. Once enabled, Location History silently collects data in the background, regardless of what a user is or is not doing on the device. This is in stark contrast to the facts in *Smith v. Maryland*, where phone users often had to interact with telephone operators using switching equipment to complete calls. *See* 442 U.S. 735, 742 (1979). Here, Mr. Chatrie could have enabled Location History by accident, just after midnight, following a long-press of the home button, after a week of annoying prompts, on a pop-up screen for Google Assistant, and bundled with other choices. If he did this, there would still be no further indication that Location History was running. Even if Mr. Chatrie never again engaged with Google's "location-based services," or any other Google service, Location History would be enabled and tracking his location at all times, even while he slept. *See supra* at 5; Tr. 122 ("[T]here were no periods of data not being collected.").

Google's Privacy Policy has little if any bearing on an individual's Fourth Amendment expectations of privacy. *See United States v. Irving*, 347 F. Supp. 3d 615, 621 (D. Kan. 2018) (rejecting government's argument that defendant had no expectation of privacy in his Facebook

account information where he agreed to Facebook's terms that "generally inform[ed] users that Facebook collects a user's content and information."); *see also Smith*, 442 U.S. at 745 (declining to "make a crazy quilt of the Fourth Amendment" based on phone company policies). It is of no assistance to the government here. First, there is no link in the "consent flow" at issue to Google's Privacy Policy, *see* Def. Ex. 7 at 1–4, a factor that courts weigh heavily when evaluating reasonable notice. *See* ECF No. 104 at 18–20; *Melo v. Zumper*, No. 3:19-cv-621 (DJN), 2020 WL 465033, at *9 (E.D. Va. Jan. 28, 2020). Second, the text of the policy was not any more illuminating than the pop-up screen. *See supra* at 19. At the time Location History was enabled on Mr. Chatrie's phone, the policy had just two lines that mention Location History. *See* Tr. 294. One line cast Location History only as a way to "save and manage location information in your account." Def. Ex. 43 at 7. The other line, in passing, states that "you can turn on Location History if you want traffic predictions for your daily commute." *Id.* at 8. These brief mentions sow only further confusion.

The government likes to point out that it was still possible to disable Location History and delete saved records. *See* Tr. 160, 416. But this assumes that Mr. Chatrie was both fully aware of the collection taking place as well as knowledgeable about how to control or stop it, and the government has offered no evidence to indicate that this was the case. On the contrary, while it is arguably too easy to enable Location History, it would have been counterintuitive and difficult for Mr. Chatrie to disable and delete, assuming he even knew about its existence.

Deleting the application from which Location History was enabled, for example, would not turn off Location History. Tr. 124; *see* Tr. 361–62. Likewise, deleting Location History data would not turn off Location History. Tr. 361. Indeed, it is telling that, once enabled, Location History can never be turned "off," only "paused." *See supra* at 14. And it is only possible to "pause" Location History by navigating through complicated settings menus and disregarding a

pop-up warning from Google that doing so will "limit[] functionality" on the device. *See id*. Similarly, while pressing "pause" means that no future data will be recorded, it does not delete any past data collected. *See supra* at 15. Even disabling Google Assistant, the app used to enable Location History here, would have no effect on either stored data or future collection. *See id*. In short, for a user to completely remove their data from the Sensorvault database, they would need to follow a specific settings permutation: a two-step process of both deleting all past Location History data and "pausing" Location History. Nowhere, not in either version of the "consent flow" or the Privacy Policy, did Google inform users of the need to take both steps or how to do them.[8]

This is not surprising, however, because Google has a clear financial incentive in increasing the number of users with Location History enabled. *See supra* at 8–9; Tr. 435–36. Google is not disinterested or neutral when presenting users with options. Rather, Google is invested in having users whose data can be used to sell lucrative advertisements that calculate rate of return by measuring "store visits." *Id*.; Tr.196–97, 301. Indeed, advertising is the main "product" that drives Google's revenue. *See* Tr. 560; *see also* Gov't Ex. 1 at 40 (showing that advertising comprised 85% of Google's revenue in 2018). In this light, the "consent flow" fits the pattern perfectly and bears a striking resemblance to lobster traps: easy to get in, hard to get out.

At the same time, Google has never been immune to public criticism, lawsuits, or regulatory action. On the contrary, Google has repeatedly received terrible headlines, civil complaints, and government inquiries over its location tracking practices, putting the company

[8] Instead, media outlets have taken on this task, publishing "how-to" articles on disabling Location History and other forms of Google location tracking. *See*, *e.g.*, Dave Johnson, *How to Stop Google from Tracking Your Android's Location*, Business Insider (Nov. 25, 2020, 9:16 AM), https://www.businessinsider.com/how-to-stop-google-tracking-android; Barbara Krasnoff, *Android 101: How to Stop Location Tracking*, Verge (Aug. 25, 2020, 3:04 PM), https://www.theverge.com/21401280/android-101-location-tracking-history-stop-how-to; Chandra Steele & Jason Cohen, *How to Get Google to Quit Tracking You*, PC Mag (Feb. 11, 2020), https://www.pcmag.com/how-to/how-to-get-google-to-quit-tracking-you; Todd Haselton, *Google Maps Tracks Everywhere You Go. Here's How to Automatically Delete What It Stores*, CNBC (Dec. 7, 2019, 9:15 AM), https://www.cnbc.com/2019/12/07/how-to-stop-google-maps-from-tracking-your-location html.

squarely on notice that its practices surrounding user consent were unacceptable and incompatible with user expectations of privacy. And in response, Google acted. *See* Def. Ex. 46; Def. Ex. 47; Tr. 260, 317, 383. Although, Google notes that it is "always looking for ways to further improve," Tr. 300, the changes Google made to Location History in this context are telling.

Since at least 2017, Google has been on notice that people found it difficult to understand how Google collects location data and what their options are. Mr. McGriff, in charge of Location History for Google since 2016, *see* Tr. 192, was acutely aware of a 2017 article in the online magazine *Quartz* as well as a 2018 article by the *Associated Press* ("AP"), both involving Location History. Tr. 220, 223–24. Both articles described Location History with alarm and were highly negative. Tr. 221–23, 225–26. The AP article made such an impression that Google prepared a report tracking how much follow-up coverage mentioned the "lack of user consent/creepy factor." Tr. 228. It also became the subject of a Monday-morning "Oh Shit" meeting for the Location History team. Tr. 248. In his defense, Mr. McGriff noted that the Google Location History team has such a meeting every Monday, which is understandable. *See id.*

It is understandable because those articles were just the beginning of the public "feedback" that Google received regarding Location History and Google's location tracking practices. *See* Tr. 218–19. Google not only became aware of the *Quartz* article, for example, but also the subsequent letter that the United States Senate to the Federal Trade Commission, urging the agency to investigate "deceptive acts and practices" associated with Location History. *See* Tr. 236; Def. Ex. 53 at 4 ("Most consumers do not understand the level, granularity, and reach of Google's data collection, and there are serious questions about whether they have provided their informed consent and maintain a reasonable ability to avoid participating in this collection."). And following the 2018 AP article, Google became aware of a class action lawsuit over its location tracking

practices. *See* Tr. 236–37. Google was also aware of a *New York Times* article revealing Google's role in geofence warrants, which in turn prompted another letter critical from Congress (this time addressed to Google's CEO). *See* Tr. 314.

Most recently, the Attorney General of Arizona filed lawsuit against Google, leading to the public release of hundreds of pages of internal emails concerning Location History. *See* Tr. 240. After publication of the AP and *Times* articles, Google employees took to company-wide email groups to express their confusion over Google's location settings. *See*, *e.g.*, Tr. 241–43, 246, 252–53, 255–56; Def. Ex. 30; Def. Ex. 31 ("Add me to the list of Googlers who didn't understand how this worked and was surprised when I read the article."); Def. Ex. 36 (explaining that Google was "trying to rein in the overall mess that we have with regards to data collection, consent, and storage"); Tr. 310–12; Def. Ex. 37 ("I'd want to know which of these options (some? all? none?) enter me into the wrongful-arrest lottery. And I'd want that to be very clear to even the least technical people.").

Regardless of the truth of these criticisms, there is no question that Google heard, discussed, internalized, and then acted on them. Public reaction was strong enough that Google made reforms to Location History, crediting this "feedback" for spurring the "auto-delete" option for Location History data. *See supra* at 15; Tr. 317; Def. Ex. 46. Google also began to send out monthly emails to users who had enabled Location History, after recognizing that users might not "understand the granularity of the data that's being collected or simply just wouldn't know . . . what exactly [Google was] collecting and how that information was being processed." Tr. 359–60. Google has no record of sending such emails to Mr. Chatrie and concedes that it may not have

sent him those emails.[9] Tr. 328; Def. Ex. 23 at 8–9. Nonetheless, these changes demonstrate that even Google knew that the "opt-in" for Location History was confusing and potentially deceptive.

D. The Third-Party Doctrine Should Not Apply Even If Mr. Chatrie Intentionally Enabled Location History.

Timothy Carpenter signed a contract with his cell phone service provider. *Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting). He did not allege that he was tricked or coerced into it. And yet, the Supreme Court still found that he was not "voluntarily" conveying his location data to the service provider, even though everyone was aware that that is how cell phones work. *Id.* at 2220 ("Cell phone location information is not truly 'shared' as one normally understands the term."). Rather than "mechanically" applying the third-party doctrine, the Court looked at the context—whether the "choice" to hand over the data truly outweighed the privacy intrusions given the realities of the digital age. *Id.* at 2219–20; *see also* ECF No. 29 at 9–11.

The Court's contextual concern exists here in abundance. "[M]echanically" applying the third-party doctrine here would divest, at a minimum, tens of millions of people of their Fourth Amendment rights merely for participating in normal everyday life. *See* Tr. 205. Google Location History may not be a pillar of digital society, but there are still "numerous tens of millions" of people who use it, wittingly or not. The *Carpenter* Court remarked on the pervasiveness of cell phones in the United States. 138 S. Ct. at 2220 (citing *Riley v. California*, 134 S. Ct. 2473, 2484 (2013)). At issue here is one-third of all Google users. It would be nonsensical to deem this data unworthy of Fourth Amendment protection unless everyone is using it, yet that is the line the government seeks to draw. Moreover, there is nothing in the government's reasoning that would limit the use of geofences to Location History data.

[9] Google also describes a "warm welcome" notification appearing in the Google Maps application, Tr. 355, but there is no indication that there was such a notification in Google Assistant, or that Mr. Chatrie received one.

Under the government's theory, people do not have an expectation of privacy in any data stored with a third-party or service provider, other than long-term CSLI. Thus, there would be nothing separating a search of Location History data from a search of Gmail users for messages mentioning a robbery of the Call Federal Credit Union. This is no mere hypothetical. Law enforcement has already forced Google to conduct reverse "keyword" searches, disclosing everyone who searched for a particular term or address.[10]

Lastly, Mr. Chatrie respectfully persists in his property-based arguments here. *See* ECF No. 29 at 14–16; ECF No. 48 at 8–10; ECF No. 109 at 20–21. Ownership is inherent in the language Google uses to describe Location History, whether telling users they are creating a "private map" of their whereabouts or calling it "your data" to delete or manage as users see fit. *See supra* at 11. Under either a property-based theory or the reasonable expectation of privacy framework set forth in *Katz*, obtaining Mr. Chatrie's Google Location History records was a Fourth Amendment search.

II. The Geofence Warrant Was an Unconstitutional General Warrant

As Mr. Chatrie has argued from the beginning, geofence warrants are inherently unconstitutional. *See* ECF No. 29 at 19–21; ECF No. 104 at 21. They are digital versions of the "dragnet" searches that Fourth Amendment was intended to prohibit. *See* ECF No. 104 at 21–24; ECF No. 29 at 16–23. The Supreme Court has never sanctioned the search of "numerous tens of millions" of people, in any context. *See* Def. Ex. 21 at 4. Additional facts from the March hearing confirm that the warrant in this case was uniquely overbroad and so lacking in particularity that it is the digital equivalent of an impermissible general warrant.

[10] Alfred Ng, *Google Is Giving Data to Police Based on Search Keywords, Court Docs Show*, CNET (Oct. 8, 2020 1:21 PM), https://www.cnet.com/news/google-is-giving-data-to-police-based-on-search-keywords-court-docs-show/.

E. Overbreadth

Overbreadth concerns probable cause, which is defined as "a fair probability" that contraband or evidence of a crime will be found in a particular place. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). A warrant is overbroad if the government lacks probable cause for the things to be searched or seized. *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). Here, the government did not have probable cause to search "numerous tens of millions" of Google accounts. It did not have probable cause to search 19 users, either, and it did not have probable cause to search nine or three. The government did not have probable cause to search even one Google account, because investigators admittedly had no suspects. Tr. 487, 637. No matter how the government seeks to dress it up in steps or stages, the complete absence of probable cause means that the warrant is fatally overbroad from beginning to end.

Step one was a dragnet, conducted by Google at the government's direction. The government made Google search through every user account with Location History enabled to identify any people within 150 meters of the Call Federal Credit Union during a 1-hour window. According to Google, this required searching "numerous tens of millions" of accounts—reviewing the contents of each one to determine if it met the government's criteria. Tr. 29, 52–53, 205; *see* Tr. 575. In other words, the government compelled Google to access "numerous tens of millions" of accounts and apply a filter of the government's peculiar design—a digital dragnet.

The warrant application provided no case-specific facts that the robber was a Google user or had Location history enabled at the time in question.[11] All the government offered was that an unknown bank robber had a cell phone and that Google tracks a lot of people's cell phones. ECF

[11] Despite "tens of millions" being an exceedingly large number, it accounts for only one-third of Google's active users. In other words, even if every cell phone user was signed into a Google account, there would only be a one in three chance of the suspect having LH enabled.

No. 109 at 14. The government contends that this is a "substantial basis" for probable cause, *id.*, but if that is true, then the government could get a geofence warrant in any investigation, simply by reciting the facts of the crime and some statistics about Google. As Mr. Chatrie has consistently argued, such broad conjecture about the popularity of Google or cell phones generally does not amount to probable cause. *See* ECF No. 29 at 23; ECF No. 48 at 19. Probable cause must be based on individualized facts, not group probabilities. *See Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). In Illinois, Judge Fuentes denied the government's application for a geofence warrant on these grounds, noting that it "resembles an argument that probable cause exists because those users were found in the place … [where] the offense happened," an argument the Supreme Court squarely rejected in *Ybarra*. *See* Fuentes Opinion, 481 F. Supp. 3d at 754.

Had the government provided a nexus between the robber and Location History, then there would have been no need to go fishing in Google's ocean of data. The government could have simply requested the Location History data for the suspect account, as it typically does. But, the government did not seek to search a particular account; it sought to search *all* accounts. That is the definition of a general warrant. *See Warden v. Hayden*, 387 U.S. 294, 313 (1967) (describing the "practice of the Star Chamber empowering a person 'to search in all places, where books were printing, in order to see if the printer had a licence; and if upon such search he found any books which he suspected to be libellous against the church or state, he was to seize them, and carry them before the proper magistrate.'").

The fact that the government's dragnet ensnared 19 people does not diminish the scope of the initial search conducted at their behest. The Fourth Amendment does not distinguish between Google and the government when it comes to conducting this initial search of millions. This case does not involve a "private search." Google did not decide on its own to search for users near the

bank, and Google never provides such information to advertisers. *See supra* at 9; Tr. 432–33. Likewise, the data produced was not an existing "business record." Google did not possess a list of people near the bank until the government required them to create one. Tr. 433. In short, Google had no independent motivation to conduct this geofence search, and Google would not have done so without a warrant. *Id.* The entire search, including the "numerous tens of millions" in step one, was conducted at the government's direction.

The government contends that this was just like a "tower dump"—another type of exceedingly broad search, the constitutionality of which is in doubt following the Supreme Court's decision in *Carpenter*. A tower dump requires cell phone service providers to produce the records of every device connected to a particular cell tower or towers during a particular time. *See* Tr. 49–50; Def. Ex. 2 at 14. Any similarity to geofence warrants, however, is merely superficial. Significantly, the number of people searched in a geofence warrant is far larger—by at least four orders of magnitude—than the number of people searched in a typical tower dump. *See* Tr. 53 (the number of people searched in a tower dump "wouldn't be close to" the number of people searched here); *see also* ECF No. 104 at 22 (surveying reported tower dump cases and finding that they tend to impact hundreds or thousands of people at most). Even the government's own hypothetical tower dump would have involved a search of roughly 3,000 people, Tr. 55, which is just a tiny fraction of the "numerous tens of millions" searched here. And more importantly, it is a long way off from a "normal Location History request for a specific account when they name the account because we know who we're looking for." Tr. at 53.

A tower dump is more limited than a geofence, relatively speaking, because cellular service providers organize, or "index" data based on location, *i.e.*, the cell towers in their networks. Unlike Google, they keep information about the use of each tower for internal business purposes, like

identifying towers that become overloaded and determining where to put up more. As a result, they are able to provide information about particular towers without searching the phone records of every customer. Google, on the other hand, indexes Sensorvault by Google account and has no way of searching by location. *See* Tr. 431–32, 572–73. The government responds that they cannot be responsible for the way Google chooses to structure its database and suggests that Google could "create an additional Location History database indexed by location" to make it easier to execute geofence warrants. ECF No. 109 at 17. But Google does not operate cell towers and has no business need to index user data in this way.

Furthermore, the warrant would still be overbroad even if it were somehow possible to restrict the initial search to devices within the geofence. The government argues that the warrant was "limited based on location, dates, and times," but the location at issue is anything but narrowly tailored. It encompasses not only the bank and parking lot, but the entire church nearby, with an effective range that included major streets, a hotel, a restaurant, other businesses, and two apartment complexes. *See supra* at 17-18. Judge Weisman recently reached this conclusion as well in denying the government's application for a geofence warrant in Illinois. *See* Weisman Opinion at *5 ("[T]he geographic scope of this request in a congested urban area encompassing individuals' residences, businesses, and healthcare providers is not 'narrowly tailored' when the vast majority of cellular telephones likely to be identified in this geofence will have nothing whatsoever to do with the offenses under investigation."). Furthermore, the government would not have had probable cause to search all 19 people who happened to be in the area. As Judge Fuentes reasoned, that data might "*include* evidence of the crime, but it will include other information as well: The location information of persons not involved in the crime." Fuentes Opinion, 481 F. Supp. 3d at 751. To justify such an "all persons" warrant, the government would have needed probable cause

that all 19 people were involved in the bank robbery. *See Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) ("[A]n 'all persons' warrant can pass constitutional muster if the affidavit and information provided to the magistrate [judge] supply enough detailed information to establish probable cause to believe that all persons on the premises at the time of the search are involved in the criminal activity."). That would have been impossible to do, of course, because the government would have had no way of knowing, *ex ante*, that there would be 19 people in the geofence.

The fact of the matter remains, however, that the step one search did not just involve 19 people, but "numerous tens of millions," none of which the government had probable cause to search. Probable cause was still absent in steps two and three, when the government seized even more Location History data from nine accounts as well as subscriber information for three of them. *See supra* at 18-19. While the government may have learned new information from the step one data it seized, the warrant application did not change and the government did not seek additional court authorization. The government lacked probable cause to search anyone's Location History, whether three, nine, nineteen, or millions. The warrant was therefore overbroad from start to finish.

F. Particularity

Particularity concerns officer discretion. Warrants must particularity describe both the place to be searched and the items to be seized in order to limit officer discretion and prevent the "exploratory rummaging" that the Framers abhorred. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *see also United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010). The particularity requirement takes on special importance where, as here, a search implicates First Amendment concerns. *See* ECF No. 104 at 24; ECF No. 29 at 13, 22; ECF No. 48 at 3 n.3. In this case, the place to be searched is the millions of accounts stored on Google's servers. The items to be seized are not specified, but instead described as the product of a three-step process that explicitly requires

the government to use its discretion. In reality, the warrant left the entire process up to Google and the government to work out internally.

The basic contours of the warrant were the product of repeated engagement between the FBI and Google. *See supra* at 4. Google decided to search Location History data, as opposed to Web & App Activity or Google Location Services data. *See id.*; Tr. 212; Def. Ex. 21 at 8. And Google picked a method of calculating which devices were inside the geofence that generated a high number of false positives—people swept up in the dragnet who were never there at all. *See supra* at 16-17. Google had to do all of this because the warrant did not specify one way or another. The issue is not whether Google should have searched other databases, or taken the Display Radius into account in its search, or whether these decisions were "correct." *See* ECF No. 109 at 18. The issue is that Google is making these decisions instead of a judge. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004). And here, these decisions had measurable consequences: At least one and as many as five of the 19 users identified in step one were likely never within the geofence, with one device that could have been more than 200 meters outside of it. *See* Tr. 42, 64, 587; ECF No. 104 at 8.

Far more troubling is the amount of discretion that the warrant envisioned for the government at steps two and three. At each step, it was up to the government to "narrow" the list of devices and determine which users will be subject to further scrutiny. Def. Ex. 1 at 4–5. Thus, in step two, the government was to decide, in some unspecified manner, which devices they would receive "contextual" data for, *i.e.*, two hours of Location History data without geographic limitation. *Id.* at 4. And in step three, the warrant left it up to the government to pick the accounts for which Google would provide full subscriber information. *Id.* at 5. This is precisely the kind of officer discretion that the particularity requirement was designed to prevent. *See* Fuentes Opinion,

481 F. Supp. 3d at 754 (finding a geofence warrant lacked particularity because it "puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information"); Weisman Opinion, 2020 WL 5491763, at *6 ("[T]his multi-step process simply fails to curtail or define the agents' discretion in any meaningful way").

Even this process, however, involved additional uncertainty and negotiation over what data the government could seize. After step one, the government repeatedly emailed and called Google to demand step-two "contextual" data, as well as step-three subscriber information on all 19 devices identified in step one. *See supra* at 18-19. It was only because Google refused that the government was unsuccessful, acquiesced, and eventually requested additional data on only nine users. *Id*. The problem is that the Fourth Amendment requires courts, not detectives or companies, to decide what the government can search and seize. Here, the warrant allowed Google and Det. Hylton to decide which accounts to search and "de-anonymize," and Det. Hylton demonstrated why the Fourth Amendment does not trust law enforcement to make that decision.

Step three similarly imbued the government with the sole discretion to decide which people would have their full subscriber information disclosed by Google. The warrant did not identify any of them, or provide any objective criteria by which to identify them. *See* Weisman Opinion, 2020 WL 5491763 at *6 ("For example, the warrant does not limit agents to only seeking identifying information as to the 'five phones located closest to the center point of the geofence,' or some similar objective measure of particularity."). Once again, the decision belonged to the government, not a court. And once again, the government used this discretion to seek additional information about one person who was likely never inside the geofence at all, something that should have been apparent from the step-two data. *See* Tr. 65–66; ECF No. 104 at 27.

At each step, the warrant allowed Google and the government to be the arbiters of what was reasonable to search and seize. No objective observer could look at the warrant and ascertain which accounts the government had authority to "de-anonymize" or obtain "contextual" about. The warrant therefore lacked particularity and violated the Fourth Amendment.

III. The Good Faith Exception Does Not Apply

The Fourth Amendment's most fundamental restraint is the warrant requirement. In *United States v. Leon*, 468 U.S. 897, 919 (1984), the Supreme Court qualified that restraint where a warrant is based on "objectively reasonable law enforcement activity." But, *Leon* "good faith" offers no qualifications in four circumstances: (1) where a warrant is based on knowing or recklessly false statements, *id.* at 914 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)); (2) where the judge acted merely as a rubber stamp for the police, *id.* (citing *Illinois v. Gates*, 462 U.S. 213 (1983)); (3) where a warrant affidavit lacks a substantial basis to determine probable cause, *id.* at 915 (citing *Gates*); and (4) where no officer could reasonably presume the warrant was valid, *id.* at 923.

The Supreme Court did not intend for the good faith exception to diminish the power and force of the Fourth Amendment. *Id.* at 924. Rather, the Supreme Court tethered the exclusionary rule to the primary tenets of the Fourth Amendment: particularity, probable cause, and a neutral magistrate who is "not [an] adjunct[] to the law enforcement team." *Id.* at 917, 923. As Mr. Chatrie has argued, *see* ECF Nos. 48 at 17-20 and 104 at 28-30, the *Leon* good faith exception to the exclusionary rule does not apply to evidence obtained from a warrant that was *void ab initio*. As set forth above and in the earlier briefing, this geofence warrant is void from its inception and is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) ("[T]he warrant was so

obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."). But, even if the Court determines that *Leon* applies here, three of the firm boundaries to the good faith rule that *Leon* recognized clearly apply.

First, the magistrate issuing the geofence warrant "abandoned his judicial role" and acted as a rubber stamp here. On June 14, 2019, the police presented the geofence warrant to a magistrate who had served for less than a year, had finished his probationary period a handful of months before, and had only a bachelor's degree from an unlicensed school. *See* ECF Nos. 135-2 at 22 and 156. There is no evidence in this case that the magistrate had any training on geofence warrants or had even seen a geofence warrant before June 14, 2019. On that date, Det. Hylton walked into the magistrate's office where other magistrates were present. Tr. 638. He handed the warrant application to Magistrate Bishop. *Id.* The magistrate looked over the application privately for maybe fifteen or thirty minutes and signed the warrant without asking a single question or making a single change to the warrant. *Id.* at 638-39. While perhaps that type of review may suffice for a more ordinary warrant, a warrant that necessarily requires governmental invasion into the intimate details of many innocent persons' private lives should generate more distress.

The magistrate's utter lack of concern regarding the obvious flaws in the warrant constituted a complete abandonment of his role as the neutral arbiter between individual privacy and government overreach. The magistrate apparently had no qualms with signing a warrant that—contrary to the Fourth Amendment's patent particularity requirement—allowed the police to search a haystack composed of numerous tens of millions of people's intimate, private data to see if a needle might turn up. The magistrate was further unconcerned that the warrant granted immense discretion to the executing officers and Google to decide what Google data to search. The affidavit in this case did not describe objectively reasonable law enforcement activity. Rather,

it described a general warrant that the framers created the Fourth Amendment to preclude. The particularity requirement "makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Stanford v. Texas*, 379 U.S. 476, 512 (1965); *see also United States v. Wilhelm*, 80 F.3d 116, 121-23 (4th Cir. 1996) (finding that magistrate acted as rubber stamp by abandoning scrutiny of basic tenet of Fourth Amendment); *United States v. Decker*, 956 F.2d 773, 777-78 (8th Cir. 1992) (finding judge did not fulfill role of neutral and detached reviewer by approving warrant with glaring omissions); *United States v. Winn*, 79 F. Supp. 3d 904, 924 (S. D. Ill. 2015) (finding judge acted as rubber stamp "when he signed off on a warrant despite the facially overbroad nature of the list of items to be seized").

Second, the good faith exception should not apply because the geofence warrant was "so lacking in indicia of probable cause" to search for Mr. Chatrie's location data that it was entirely unreasonable for any objective officer—i.e., one who had even a rudimentary understanding of the Fourth Amendment's particularity and breadth requirements—to rely on. *See Leon*, 468 U.S. at 923. Here, police knew a robbery suspect was carrying what appeared to be a cell phone. Tr. 608. They had no idea what company made the cell phone, what carrier provided service for the phone, what operating system the phone used, or what applications and permissions were installed and actively gathering data on the phone. Rather than trying to do some detective work like track down the owner of the car the suspect was seen in and compare that information to cell phone numbers that had connected with a nearby cell phone tower, Tr. 578-79, the police decided to get permission to rummage through numerous tens of millions of people's location data simply because the robbery suspect had what appeared to be a cell phone in his hand.

Police must demonstrate a fair probability that the evidence the police seek will be where they are searching. *See United States v. Doyle*, 650 F.3d 460, 472 (2011) (rejecting good-faith exception where warrant application contained "remarkably scant evidence . . . to support a belief that [the defendant] *in fact* possessed child pornography"); *see also United States v. Church*, 2016 WL 6123235, at *6-7 (E.D. Va. Oct. 18, 2016) (observing that good-faith exception inappropriate where no evidence to connect suspect's house to the crime under investigation); *United States v. Shanklin*, 2013 WL 6019216, at *9 (E.D. Va. Nov. 13, 2013) ("A reasonable police officer would be unable to infer through normal inferences that electronic devices owned by child abusers in general or the Defendant specifically contain evidence related to the criminal activity being investigated . . . ."). That did not happen here. Rather, what happened here was the police obtained a warrant based on conjecture that Google had location data for the cell phone the robbery suspect appeared to be carrying. Obtaining warrants based on conjecture is certainly not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

Third, the good faith exception should not apply because the geofence warrant was "facially deficient" and no objective officer could reasonably presume it was valid. *See Leon*, 468 U.S. at 923. As an initial matter and as set forth above, "it is obvious that a general warrant authorizing the seizure of 'evidence' without [complying with the particularity requirement] is void under the Fourth Amendment" and "is so unconstitutionally broad that no reasonably well-trained police officer could believe otherwise." *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992); *see also United States v. Leary*, 846 F.2d 592, 607-09 (10th Cir. 1988) ("reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized," and collecting like cases from the First, Eighth, and Ninth Circuits).

Additionally, the extraordinary discretion this warrant purported to authorize renders the warrant facially deficient. Law enforcement agencies and Google worked hand-in-hand in to develop the three-step process outlined above for requesting and responding to geofence warrants. Tr. 455-57, 476. Google, sometimes with police help, gets to decide how big of a geographical area is too big. Tr. 455-58, 461. Google, sometimes with police help, gets to decide if a range of time is too long. Tr. 458-59, 462-64. Google also gets to decide if it does not want to comply with a geofence warrant because it is too sensitive, say for political reasons. Tr. 459-60. Google gets to decide any time limits it wants to apply in between the various steps in the three-step process. Tr. 464-66, 469-70. Google gets to decide if the police have attempted to narrow the information to be seized between the various stages. Tr. 467-69, 471-72. In sum, the three-step process that law enforcement agencies and Google created for Google to respond to geofence warrants entrusts essentially unfettered discretion with the police and Google to execute the warrant.

While Det. Hylton had no training in understanding or applying for geofence warrants, Tr. 627-28, no objective officer could have reasonably believed that a warrant that gave Google and the police unprecedented discretion in executing the warrant was valid. *See George*, 975 F.2d at 76 ("Absent some limitation curtailing the officers' discretion when executing the warrant, the safeguard of having a magistrate determine the scope of the search is lost."); *Leary*, 846 F.2d at 609 ("A warrant that directs an officer to seize records 'relating to' violations of the federal export laws offers no such guidelines. The officers were left to their own discretion."); *see also Winn*, 79 F. Supp. 3d at 924 ("it was not objectively reasonable for the[police] to think that a warrant was valid when it gave them unbridled discretion to search for and seize whatever they wished"). Obtaining warrants authorizing nearly unfettered discretion is certainly not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

For any of these reasons, the Court cannot find that the good-faith exception applies to evidence that the government obtained from the geofence warrant and the fruits flowing therefrom. While Mr. Chatrie has not and is not raising a *Franks* claim, the misleading information in the warrant application and material information the police omitted from the warrant certainly reinforces the conclusion that the Court should not apply the good-faith exception in this case. *See Leary*, 846 F.2d at 609-10 (finding that conduct and circumstances of the search reinforced conclusion that "suppression of the evidence is appropriate to deter government misconduct"). In this case, the government falsely told the magistrate that the Google data in the first two stages was anonymous. We know now that a person can reasonably be identified through a handful of location points. Tr. 62-70; ECF 104 at 12; 1/21/20 Tr. at 83, 87-88, 90-91. The Device ID Google uses to identify a device and account remains the same from warrant to warrant. Tr. 451-54. The police did not inform the magistrate that Google would have to search numerous tens of millions of people's private location diaries in stage one. The police also did not inform the magistrate that the geofence would almost certainly capture devices outside of the geofence or that the approximate device locations were only 68% accurate. This level of misinformation and omitted information only underscores that the geofence warrant in this case was not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

CONCLUSION

If ever there were a case to find that the government used a general warrant, then this is it: a dragnet of "numerous tens of millions" paired with unchecked discretion. The warrant was so profoundly overbroad and lacking in particularity that the good faith doctrine should not apply. Mr. Chatrie therefore asks this Court to suppress all evidence obtained from geofence warrant and all of its poisonous fruits.

Respectfully submitted,
OKELLO T. CHATRIE

By: /s/

Michael W. Price
NY Bar No. 4771697 (*pro hac vice*)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

/s/
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

/s/.
Paul G. Gill
Va. Bar No. 31461
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0870
Fax (804) 648-5033
Paul_gill@fd.org

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE IN OPPOSITION TO
DEFENDANT'S MOTION FOR SUPPRESSION

When someone robbed the Call Federal Credit Union in Chesterfield, Virigina, Google was a witness. Defendant Okello T. Chatrie had chosen to have Google keep a record of where he went with his cell phone in order for Google to provide him with location-based services. As a result, evidence of the defendant's presence at the bank robbery was stored in a database that Google accesses freely to provide services to its users and advertisers. A Virginia magistrate determined that there was probable cause to believe that Google possessed evidence of the robbery, and he issued a geofence search warrant.

The warrant authorized disclosure from Google of two hours of location information associated with electronic devices that were, over a one-hour interval, within 150 meters of the site of the bank robbery. Pursuant to the warrant, Google produced location information over a two-hour interval of three subsequently identified and six unidentified individuals, and limited location information over a one-hour interval of ten other unidentified individuals. From this information, investigators identified the defendant and solved the robbery.

In his post-hearing brief, the defendant continues to argue that this evidence should be

suppressed, but this Court should deny the defendant's motion to suppress for three separate and independent reasons. *See* Def.'s Post-Hearing Mot. To Suppress, ECF No. 203, (hereinafter, "Def. Post-Hr'g Suppl. Br."). First, the government did not conduct a search under the Fourth Amendment when it obtained this location information from Google. Second, the geofence warrant complied with the Fourth Amendment, as it was based on probable cause and specified its object with particularity. Third, suppression is inappropriate because investigators relied on the warrant in good faith.

I. STATEMENT OF FACTS

A. The Robbery and the Geofence Warrant

At approximately 4:50 pm on May 20, 2019, a then-unknown male entered the Call Federal Credit Union in Midlothian, Virginia. *See* Geofence Search Warrant, Gov't Ex. 2, at 6 (hereinafter, "Gov't Ex. 2")[1]; Motion to Suppress Hearing Transcript, ECF Nos. 101, 102, at 608 (hereinafter, "Suppression Hr'g Tr."). With his right hand, the robber held a cell phone to his face and appeared to be speaking to someone. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 608. He approached a teller and presented a note that read, in part, "I got your family as hostage and I know where you live, If you or your coworker alert the cops or anyone your family and you are going to be hurt. . . . I need at least 100k." Gov't Ex. 2 at 6; Suppression Hr'g Tr. 608-09. After the teller replied that she did not have access to that amount of money, the robber pulled out a silver and black firearm. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 609. After first forcing everyone to the ground at gunpoint, the robber escorted the manager and others to the back of the business where the vault was located. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 608-09. The robber forced the manager to open the safe

[1] Page numbers for Government Exhibit 2 refers to the numbering in red at the bottom of each page. Such numbering is consistent where an exhibit of the United States has red numbering at the bottom.

and place $195,000 into a bag. Gov't Ex. 2 at 6. The robber then fled towards a church west of the bank. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 609-10.

Federal Bureau of Investigation Task Force Officer ("FBI TFO") Josh Hylton responded to the scene to investigate. Suppression Hr'g Tr. 607. From the fact that the robber had carried a phone, FBI TFO Hylton knew that there was a possibility that the robber might have had a lookout or a driver nearby. Suppression Hr'g Tr. 610.

FBI TFO Hylton also knew that Google could have data that would show the robber was in the area at the time of the robbery. Suppression Hr'g Tr. 610. On three prior occasions, FBI TFO Hylton had obtained geofence warrants directed to Google. Suppression Hr'g Tr. 603. Moreover, he had consulted with prosecutors prior to obtaining the geofence warrants. Suppression Hr'g Tr. 604. One was issued by a United States Magistrate Judge, and two were issued by Virginia state judges. Suppression Hr'g Tr. 603-04. In seeking these warrants, he had never been told that geofence warrants were not legal. Suppression Hr'g Tr. 604-05.

On June 14, 2019, FBI TFO Hylton sought and obtained a geofence warrant from the Chesterfield Circuit Court of Virginia. *See* Gov't Ex. 2. His statement of probable cause began by describing the facts of the robbery, including that prior to the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone. Gov't Ex. 2 at 6. The statement then explained why there was reason to believe that Google would have evidence pertaining to the robbery. Gov't Ex. 2 at 7. Among other facts, the statement disclosed: (1) that as of 2013, 56% of cell phones were smartphones; (2) that "[n]early every" Android phone "has an associated Google account"; (3) that Google "collects and retains location data" from such devices when the account owner enables Google location services; and (4) that Google collects location information from non-Android smartphones if the devices are "registered to a Google account and the user has

location services enabled." Gov't Ex. 2 at 7. Magistrate David Bishop issued the geofence warrant upon a finding of probable cause. *See* Gov't Ex. 2 at 8.

The geofence warrant specified a target geographical area, identified as a circle of radius 150 meters around a specific latitude and longitude point west of the bank, such that the circle covered both the bank and the place where the robber parked. Gov't Ex. 2 at 5; Suppression Hr'g Tr. 523. It authorized disclosure of location information over a two-hour interval (from 3:50 pm to 5:50 pm) from accounts associated with devices within this target area at some point during a one-hour interval that included the robbery (from 4:20 pm to 5:20 pm). Gov't Ex. 2 at 4-5. The warrant also authorized disclosure of specified customer identity information associated with these accounts, including user name and email address. Gov't Ex. 2 at 4-5.

The warrant authorized this disclosure through a three-step process that enabled law enforcement to "narrow down" the information disclosed by Google and thus obtain less than the maximum amount of information covered by the warrant. Gov't Ex. 2 at 4-5. The warrant directed that in the first step, Google was to disclose anonymized location for devices present in the target area during the hour of the robbery, but not the identity information associated with the devices. Gov't Ex. 2 at 4. In particular, the warrant directed that Google disclose "a numerical identifier for the account, the type of account, time stamped location coordinates and that data source that this information came from if available." Gov't Ex. 2 at 4.

In the second step, law enforcement was to review the anonymized location information produced by Google and identify the accounts of interest, and Google was then to disclose location information for those accounts over the full two-hour interval, both within and outside of the target area, but again without disclosing user identity information. Gov't Ex. 2 at 4-5. In the third step, law enforcement was to identify accounts that remained of interest, and Google was to disclose

user name and other specified subscriber identity information for those accounts. Gov't Ex. 2 at 5.

Investigators followed this three-step process in executing the warrant. Suppression Hr'g Tr. 533-50. In the first phase, Google provided 209 data points concerning 19 accounts (including 38 points from the defendant's account), all within the 150 meter circle and during the hour of the bank robbery. *See* FBI Cellular Analysis Survey Team, Gov't Ex. 1, at 20, 22 (hereinafter, "FBI CAST Report"); Suppression Hr'g Tr. 534-35; *see also* Sealed PDF of Raw Data, Def. Ex. 3. For each data point, Google produced an account ID, date and time, latitude and longitude coordinate, source of information (wi-fi or GPS), and "map display radius." *See* FBI CAST Report at 17-22. "Map display radius" is a measure of Google's confidence in the accuracy of its location information; Google's aim is to capture roughly 68% of users within the circle defined by its location estimate and the map display radius. Suppression Hr'g Tr. 213-14; *see also* McGriff Decl. dated Mar. 11, 2020 at ¶¶ 24-25 (ECF No. 96-1), Gov't Ex. 3, (hereinafter, "Gov't Ex. 3").

By reviewing the phase 1 data in conjunction with witness interviews and video surveillance tapes, investigators concluded that the defendant's device likely belonged to the robber. Suppression Hr'g Tr. 549-50.

In the second phase, FBI TFO Hylton initially asked Google for data regarding all 19 accounts, but Google was nonresponsive. Suppression Hr'g Tr. 622; Email Correspondence between FBI TFO Hylton and Google, Gov't Ex. 4 at 4. Concerned about the dangerousness of the situation, FBI TFO Hylton called Google, and he ultimately narrowed the second-stage production to nine accounts. Suppression Hr'g Tr. 622, 642; Gov't Ex. 4 at 9. Google produced two hours of location data for each of these accounts—a total of 680 data points, including 94 data points for the defendant's account with a device ID ending in 5659. FBI CAST Report at 26.

In the third phase, FBI TFO Hylton directed Google to disclose subscriber information for three accounts, including the account of the defendant. Suppression Hr'g Tr. 543. This information included the defendant's email address. Suppression Hr'g Tr. 544.

Location History information is the only information stored by Google that can be responsive to a geofence warrant because it is the only information stored by Google that is associated with specific users and sufficiently granular to be responsive. *See* Gov't Ex. 3 at ¶ 20; Suppression Hr'g Tr. 378-79. To identify responsive information, Google runs a computation against all stored Location History coordinates to determine which ones match the geofence parameters. *See* Gov't Ex. 3 at ¶ 20. It would be technically possible for Google to index its Location History database by user location rather than user accounts. Suppression Hr'g Tr. 402-03.

B. The Defendant's Google Account

On August 20, 2017, the defendant created the email account Okellochatrie55@gmail.com. McGriff Decl. dated Aug. 7, 2020 at ¶ 2 (ECF No. 171-1) & Gov't Ex. 3c at Exhibit A (hereinafter, Gov't Ex. 3c). At that time, he agreed to Google's terms of service. Suppression Hr'g Tr. 382. Those terms specified that "[b]y using our Services, you agree that Google can use such data in accordance with our privacy policies." See Google Terms of Service last modified October 25, 2017 at 3, Gov't Ex. 5a, (hereinafter, "Gov't Ex. 5a"). [2]

On July 9, 2018, the defendant opted in to Google's storage of his Location History. Gov't Ex. 3c at ¶ 5 & Exhibit B. Google Location History allows users "to keep track of locations they

[2] The terms of service available at that time are also available at https://policies.google.com/terms/archive/20140414. The best evidence of Google's privacy policy and terms of service is online. Suppression Hr'g Tr. 386.

have visited while in possession of their compatible mobile devices." Gov't Ex. 3 at ¶ 4. Google uses Location History to provide location-based services to users: for example, users can obtain "recommendations based on places they have visited, get help finding their phones, and receive real-time traffic updates about their commutes." Gov't Ex. 3 at ¶ 6; Suppression Hr'g Tr. 292, 347.

Google also uses Location History for advertising purposes. Gov't Ex. 3 at ¶¶ 5, 14; Suppression Hr'g Tr. 196-98, 561. It infers users' interests from where they visit, and it uses that "semantic location information" to target advertising to users. Gov't Ex. 3 at ¶¶ 5, 14. Google also targets ads to users based on their proximity to a particular business. Suppression Hr'g Tr. 198. In addition, Google uses location information to measure "store visit conversions"—how many customers who saw a particular ad went on to visit a relevant store. Gov't Ex. 3 at ¶ 14; Suppression Hr'g Tr. 196-97. Although Google does not share a user's Location History directly with advertisers, it does share with advertisers store visit conversion information that it derives from Location History. Suppression Hr'g Tr. 196-97, 561.

The majority of Google users decline to opt in to Location History. Suppression Hr'g Tr. 351. In 2019, approximately one-third of active Google users had Location History enabled. Gov't Ex. 3 at ¶ 13; Suppression Hr'g Tr. 387.

A Google user may review, edit, or delete Location History information. Gov't Ex. 3 at ¶ 15; Suppression Hr'g Tr. 321, 388, 416. Deletion takes place nearly immediately. Suppression Hr'g Tr. 416. Deleted Location History information is not retained at all, even in anonymized form. Suppression Hr'g Tr. 321. A Google user may also stop collection of Location History information. Suppression Hr'g Tr. 416. Stopping collection can be accomplished through any of three paths: settings on any App that uses Location History, device-level settings, or through the

myactivity.google.com website. Suppression Hr'g Tr. 340-41.

Opting in to storage of Location History is not the only step a user must take in order for Google to store the user's Location History. Gov't Ex. 3 at ¶¶ 7-11. As Location History Product Manager Marlo McGriff explained, Location History "functions and saves a record of the user's travels only when the user opts into [Location History] as a setting on her Google account, enables the 'Location Reporting' feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it." Gov't Ex. 3 at at ¶ 10.[3]

When the defendant opted in to Location History on July 9, 2018, a user could not opt in to storage of Location History without following Google's "supported consent flow," which is "the steps and consent text necessary to opt in" to its service. Gov't Ex. 3c at ¶ 6. If a user attempted to opt in using an unsupported consent flow, the process would not be successful. Suppression Hr'g Tr. 297. Under the supported consent flow for Location History on July 9, 2018, Google presented the user with the following text:

> **Location History**
>
> Saves where you go with your devices
>
> This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

Gov't Ex. 3c at ¶ 7.

[3] In his testimony at the suppression hearing, McGriff affirmed that he stood by his affidavits. Suppression Hr'g Tr. 376.

Along with this text, Google presented an expansion arrow to the user that the user could tap to obtain additional information about Location History. Gov't Ex. 3c at ¶ 8. This expanded Location History text stated:

> **Location History**
>
> Saves where you go with your devices
>
> Location History saves where you go with your devices. To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, like Google Maps or Search.
>
> If you use your device without an internet connection, your data may be saved to your account once you return online.
>
> Not all Google services save this data to your account.
>
> This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google.
>
> This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

Gov't Ex. 3c at ¶ 8.

Regardless of the Application or service a user was using, a user could not opt in to Location History on July 9, 2018, without encountering this consent flow text and tapping "TURN ON." Gov't Ex. 3c at ¶¶ 10-11.

Defense expert Spencer McInvaille determined that he could not "replicate the opt-in process [for Location History] Mr. Chatrie would have seen." McInvaille Suppl. Report, Def. Ex. 7, at 1 (hereinaifter, "Def. Ex. 7"); Suppression Hr'g Tr. 152. From his analysis of the defendant phone, McInvaille believed that the defendant installed Google Assistant shortly before he opted

in to Location History. Suppression Hr'g Tr. 76. McInvaille opined that the defendant had used Google Assistant to activate Location History. Suppression Hr'g Tr. 79.

McInvaille then looked for publicly available information regarding past use of Google Assistant to opt in to Location History. Def. Ex. 7 at 1; Suppression Hr'g Tr. 82. He found three examples, but only his third came from the time frame when the defendant opted in to Location History. Def. Ex. 7 at 1-4. His first example is an article that appeared at qz.com on January 24, 2018, nearly six months before the defendant opted in to Location History. Def. Ex. 7 at 1; Suppression Hr'g Tr. 220. That article includes a screenshot showing some opt-in language for Location History, but the language shown does not follow the supported consent flow required by Google to opt-in on July 9, 2018. Def. Ex. 7 at 1. For example, rather than saying "Saves where you go with your devices", it says "Creates a private map of where you go with your signed-in devices." Def. Ex. 7 at 1.

Second, McInvaille found an Oracle report dated September 2018. Def. Ex. 7 at 2; Oracle Report dated September 2018, Def. Ex. 11 at 4 (hereinafter, "Def. Ex. 11"). The Oracle report also includes screenshots capturing some opt-in language for Location History, but it does not identify when its screenshot were taken, and the language from the screenshots again does not follow the supported consent flow required by Google to opt in on July 9, 2018. Def. Ex. 7 at 2; Def. Ex. 11 at 4. For example, like the qz.com article, the screenshot states: "Creates a private map of where you go with your signed-in devices." Def. Ex. 7 at 2; Def. Ex. 11 at 4.

Third, McInvaille found a report from the Norwegian Consumer Council with screenshots taken approximately contemporaneously with when the defendant opted in to Location History. Def. Ex. 7 at 3-4. In particular, the Norwegian reports includes screenshots taken on July 2 and August 9, 2018. *Id.* The screenshots in the Norwegian report are consistent with the supported

consent flow set forth by McGriff: every word of the supported consent flow set forth by McGriff is visible in the Norwegian screenshots. Gov't Ex. 3c at ¶¶ 7, 8; Def. Ex. 7 at 3-4. McInvaille believed that the Norwegian report captures "the true depiction of the opt-in process." Suppression Hr'g Tr. 100.

The Google Assistant process varied based on a user's previous use of Google's products and services. Suppression Hr'g Tr. 415. The screenshots from the Norwegian report showed opt-in text for Location History bundled with opt-in language for Device Information and Voice and Audio Activity. Def. Ex. 7 at 3-4. However, a user who had previously consented to Device Information and Video and Audio Activity would see only Location History. Suppression Hr'g Tr. 335. The record does not indicate whether the defendant opted in to any other Google services at the time he opted in to Location History.

Google's Privacy Policy provided further information to Google users regarding Google's storage and use of location information. Google Privacy Policy effective January 22, 2019, Gov't Ex. 5 (hereinafter, "Gov't Ex. 5"). The Privacy Policy in effect on the date of the robbery—May 20, 2019—included the following:

> We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you. . . .
>
> The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices. . . .
>
> We use the information we collect in existing services to help us develop new ones. . . .
>
> For example, you can turn on Location History if you want traffic predictions for your daily commute.

Gov't Ex. 5 at 4-6, 9. The Privacy Policy also explained to users multiple mechanisms for deleting their data, including deleting specific data and deleting data from specific services. Gov't Ex. 5 at 11-12.

II. ARGUMENT

A. *The Defendant Had No Reasonable Expectation of Privacy in Two Hours of the Location Information He Disclosed to Google.*

The defendant had no reasonable expectation of privacy in any of the information disclosed by Google pursuant to the geofence warrant. This result is hardly surprising: to obtain location-based services, a user must disclose his location to the service provider. Thus, the government's acquisition of two hours of the defendant's location information is governed by the long-standing principle that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *United States v. Miller*, 425 U.S. 435, 443 (1976). In addition, the defendant has no reasonable expectation of privacy in his location information under *Carpenter v. United States*, both because *Carpenter* retained the third-party doctrine and because *Carpenter* held only that the government infringes a cell phone owner's reasonable expectation of privacy when it accesses seven days or more of cell phone location information. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 n.3, 2220 (2018).

1. The Fourth Amendment does not protect information disclosed to a third party and then conveyed by the third party to the government.

In cases ranging from private conversations to business records, the Supreme Court has repeatedly held that the Fourth Amendment does not protect information revealed to a third party and then conveyed by the third party to the government. This principle applies to statements made in the presence of an informant. *See Hoffa v. United States*, 385 U.S. 293, 302 (1966). It applies to information disclosed to an accountant. *See Couch v. United States*, 409 U.S. 322, 335-36

(1973). It applies to bank records. *See United States v. Miller*, 425 U.S. 435, 443 (1976). It applies to dialed telephone number information. *See Smith v. Maryland*, 442 U.S. 735, 742-44 (1979). It applies to financial records. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984). And in this case, this principle applies to two hours of location information disclosed to Google to obtain location-based services.

In addition to its broad scope, the principle that the government may obtain information revealed to a third party has deep roots. The Supreme Court has recognized that "as early as 1612, . . . Lord Bacon is reported to have declared that 'all subjects, without distinction of degrees, owe to the King tribute and service, not only of their deed and hand, but of their knowledge and discovery.'" *Blair v. United States*, 250 U.S. 273, 279-280 (1919) (quoting *Countess of Shrewsbury Case*, 2 How. St. Tr. 769, 778 (1612)). Similarly, the Court has recognized that it is an "ancient proposition of law" that the public "has a right to every man's evidence." *United States v. Nixon*, 418 U.S. 683, 709 (1974). In this case, Google was a witness to the robbery: it had information regarding the bank robbery in a database which it accessed and used to provide services to its users and advertisers. The public had a right to Google's evidence, and the Fourth Amendment did not bar the United States from obtaining that evidence from Google.

2. The defendant voluntarily conveyed his location information to Google.

A closer look at Google's location-based services, its opt-in process, and its agreements with the defendant all confirm what Google told this Court: that Google users "voluntarily choose to save and share [Location History] information with Google." ECF No. 59 at 22.

a. Google's location-based services

As an initial matter, the fact that the defendant voluntarily disclosed his location to Google is evident from the nature of the relationship between Google and its users: users provide their

location to Google in order to receive location-based services. Courts often infer that an individual voluntarily disclosed information to a third party based on the nature of the relationship between the individual and the third party. For example, in *Miller*, the Supreme Court did not need to consider Miller's explicit agreements with his bank in order to conclude that he had voluntarily disclosed his financial information. Instead, the Court's conclusion was based on "examin[ing] the nature of the particular documents sought" and concluding that they were "not confidential communications but negotiable instruments to be used in commercial transactions." *Miller*, 425 U.S. at 442.

Google customers disclose their location to Google to obtain services that depend on Google knowing their specific location, such as mapping, traffic updates, help finding their phones, and help with their commutes. Gov't Ex. 3 at ¶ 6; Suppression Hr'g Tr. 347; Gov't Ex. 3c at ¶ 8. Google also uses location information to target advertisements to users, both through users' current location and based on inferences Google draws from Location History. Gov't Ex. 3 at ¶ 5, 14; Suppression Hr'g Tr. 198. In addition, Google uses location information to measure "store visit conversions," which it shares with advertisers. Suppression Hr'g Tr. 196-97.

All of these services demonstrate that Google does more than provide a mere storage service for location information. Based on a user's location, Google provides services that are helpful to the user, like mapping or finding a phone. It uses location information to provide services that are helpful to both the user and other users in the area, like traffic updates. And Google's advertising services employ user location information to benefit the user, the advertiser, and Google itself. In sum, a user of Google's location services does not keep his location private; a user shares location information with Google to obtain location-based services. Because "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and

conveyed by him to Government authorities," *Miller*, 425 U.S. at 443, the government did not infringe the defendant's Fourth Amendment interests when it obtained location information he disclosed to Google.

Furthermore, the fact that Google does not normally share a user's specific location directly with additional parties does not affect this analysis. As the Supreme Court stated in *Miller*, the third-party doctrine applies to information disclosed to a third party even "if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Miller*, 425 U.S. at 443. Here, the United States did not infringe the defendant's Fourth Amendment interests because he disclosed his location to Google; the extent to which Google shares that information with others does not change this result.

b. Google's opt-in process

The opt-in process necessary for Google to store the defendant's Location History further demonstrates that the defendant voluntarily disclosed his location to Google. Unlike a phone company's collection of cell-site information, Google would not have obtained the defendant's location information during the bank robbery unless the defendant had taken the multiple steps necessary to enable him to share his location with Google. Google saves Location History "only when the user opts into [Location History] as a setting on her Google account, enables the 'Location Reporting' feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it."

Gov't Ex. 3 at at ¶ 10.[4]

McGriff also specified the supported consent flow necessary for the defendant to store his Location History. Gov't Ex. 3c at ¶¶ 7, 8. The text of this consent flow establishes that the defendant voluntarily disclosed his location information to Google.

As an initial matter, the record makes clear that the consent flow language that the defendant agreed to is the consent flow language set forth in the McGriff affidavit. Gov't Ex. 3c at ¶ 7-8. McGriff swore that this language was used "across all applications and services, and across all Android devices and operating systems" on July 9, 2018, when the defendant opted in to Location History. Gov't Ex. 3c at ¶ 7. Moreover, every word of this language appears in the contemporaneous Norwegian report cited by the defendant, which states that its screen shots were taken in July and August of 2018. Gov't Ex. 3c at ¶ 7, 8; Def. Ex. 7 at 3-4. In contrast, the qz.com article comes from January 2018, and the Oracle report does not document when its screenshots were taken, but it has language similar to the qz.com article. Def. Ex. 7 at 1-2; Def. Ex. 11 at 4.

Thus, when the defendant argues based on language from the qz.com article, such as his repeated references to Google referring to Location History as creating a "private map," he is arguing based on opt-in language that Google did not present to the defendant during the opt-in process. Def. Post-Hr'g Suppl. Br. at 24, 32. Had defendant not encountered the supported consent

[4] The defendant claims that this process "boiled down to a single pop-up screen in Google Assistant," but his claim is not supported by the record. Def. Post-Hr'g Suppl. Br. at 24. The defendant's own expert conceded that he could not replicate the defendant's opt-in process. Suppression Hr'g Tr. 152. Only McGriff provided sworn testimony regarding all the steps of the opt-in process. Gov't Ex. 3 at at ¶ 10. Moreover, it is clear that the "single pop-up screen in Google Assistant" could not have done everything necessary for Google to store the defendant's Location History. For example, prior to that screen, the defendant would have had to sign into his Gmail account Okellochatrie55@gmail.com using his phone. The defendant may have used Google Assistant, but he still needed to complete all the steps described by McGriff in order for Google to store his Location History.

flow language, his attempt to opt in to Location History would have failed. Gov't Ex. 3c at ¶ 6. This Court should disregard arguments based on language from outside the supported consent flow presented to users on July 9, 2018.

The language from the supported consent flow of July 9, 2018, confirms that the defendant voluntarily disclosed his location to Google. Google informed the defendant that Location History "[s]aves where you go with your devices" and that "[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com." Gov't Ex. 3c at ¶ 7. This language was concise, accurate, and easy to understand, and it set forth the core components of Google's Location History service: that Google would store the defendant's location information and that Google would use that information to provide services to the defendant. It also informed the defendant that he could see and delete his information through the Google website. *See id.* In addition, Google provided the defendant with the opportunity to obtain more detailed information concerning Location History by clicking an expansion arrow. Gov't Ex. 3c at ¶ 8. After Google presented this text to the defendant, he tapped "TURN ON." Gov't Ex. 3c at ¶ 10. This opt-in process establishes that the defendant voluntarily disclosed his location to Google.

The defendant makes numerous objections to this opt-in language, but his objections cannot obscure the fundamental fact that he agreed that Google would save his Location History and use it to provide him services. His objections therefore do not withstand scrutiny.

First, the defendant objects that "a user might reasonably infer that this 'private map' or saved data would be saved only on their device, not with Google." Def. Post-Hr'g Suppl. Br. at 25. Not only did Google not refer to a "private map," and not only is the storage location of data disclosed to Google to obtain Google services of no significance, but also Google's concise

consent-flow language made clear that the defendant's location data would be stored remotely: Google informed the defendant that he could review or delete his data "at account.google.com." Gov't Ex. 3c at ¶ 7. Google's use of this URL confirms that the data is stored remotely by Google, not on the user's device. In addition, via the expansion arrow, Google further informed potential Location History customers that "[t]o save this data, Google regularly **obtains location data from** your devices." Gov't Ex. 3c at ¶ 8 (emphasis added). Google informed the defendant that his data would be stored remotely.

Second, the defendant objects that Google did not inform users "about the frequency or sheer quantity of data collected." Def. Post-Hr'g Suppl. Br. at 26. The Supreme Court, however, has made clear that this objection lacks constitutional significance. In *Smith v. Maryland*, 442 U.S. at 745, the Court held that a phone company's choices regarding storage of dialed telephone number information did not "make any constitutional difference" because the defendant "voluntarily conveyed to it information that it had facilities for recording and that it was free to record." Here, the defendant similarly conveyed his location information to Google, and Google's decisions regarding how often to store that information lack constitutional significance. Moreover, Google did not mislead the defendant in any way. Google did exactly what the defendant agreed it should do: store where he went with his device. Because people often move fast and do not stay in one place for long, relatively frequent storage of location information by Google is necessary for it to provide quality service. Furthermore, Google informed the defendant that he could review his stored data at account.google.com. Thus, if he wanted to know more about how frequently Google stored his location, that information was available to him there.

Third, the defendant objects that "nothing explains that Location History will operate independently, regardless of whether the phone is in use." Def. Post-Hr'g Suppl. Br. at 26. Again,

this objection is based on a misinterpretation of Google's consent flow language. Google's concise explanation of its service stated that Location History "[s]aves where you go with your devices." Gov't Ex. 3c at ¶ 7. This categorical language includes no limitations or exceptions, thereby making clear that the Location History service did not depend on use of specific Apps. The defendant is essentially suggesting that Google should have added redundancy to Google's concise consent flow language, but redundancy was not required for the defendant to voluntarily disclose his location to Google. In addition, Google's expanded consent flow language stated that "[t]his data is saved even when you aren't using a specific Google service." Gov't Ex. 3c at ¶ 8.

Fourth, the defendant objects that "it would have been counterintuitive and difficult for Mr. Chatrie to disable and delete [his Location History], assuming he even knew about its existence." Def. Post-Hr'g Suppl. Br.at 27. But Google did not keep secret the data or the defendant's ability to delete it. It informed him: "You can see your data, delete it and change your settings at account.google.com." That language was more than sufficient to inform the defendant of his ability to delete information and where to find the details on how to do so. The defendant also seems to suggest that the distinction between deleting data and halting its future collection is hopelessly complicated, but nothing in that distinction is particularly confusing. On the contrary, given the defendant's ability to review his data at account.google.com, it would have been easy for him to confirm that he had, in fact, deleted his data.

In sum, the defendant's objections to Google's consent-flow language are premised on the notion that Google should have presented the defendant with a longer description of its service, rather than including the longer description through an optional expansion arrow. But Google's actual approach—concise text informing the defendant that it would save his location information and use it to provide him services, along with an expansion arrow linking to more detailed

information—is sufficient to establish that the defendant voluntarily disclosed his location information to Google. At the evidentiary hearing, McGriff explained the practical result of the defendant's approach: a "wall of text" that users would not be inclined to read. Suppression Hr'g Tr. 441.[5]

c. Google's Privacy Policy

Finally, Google's Privacy Policy further supports the fact that the defendant voluntarily disclosed his location information to Google. Courts rely on terms of service and privacy policies in evaluating whether a service provider's disclosure of information to the government violates the Fourth Amendment. *See, e.g.*, *United States v. Adkinson*, 916 F.3d 605, 610 (7th Cir. 2019) (holding that that T-Mobile's disclosure of cell-site information to the government did not violate Adkinson's Fourth Amendment rights because Adkinson "agreed to T-Mobile's policy that T-Mobile could disclose information when reasonably necessary to protect its rights, interests,

[5] The defendant points to criticism of Google's Location History service from other parties, *see* Def. Post-Hr'g Suppl. Br. at 29-30, but this Court should give such criticism no weight. First, this Court did not admit that criticism for the truth of the matter asserted. Second, the record in this case sets forth the actual consent flow language Google presented to the defendant. Thus, there is no need for this Court to defer to the views of various third parties about Google's opt-in procedures—views potentially based on different language than that actually presented to the defendant. In addition, those critics are not attempting to address the question before this Court: whether, for Fourth Amendment purposes, the defendant voluntarily conveyed his location information to Google.

property, or safety").[6] Here, through Google's Terms of Service, the defendant agreed that Google could use his information in accordance with its Privacy Policy. Suppression Hr'g Tr. 382; Gov't Ex. 5a at 3. And that Privacy Policy stated: "We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you." Gov't Ex. 5 at 4. In addition, the Privacy Policy contained specific examples pertaining to Location History, including: "you can turn on Location History if you want traffic predictions for your daily commute." *Id.* at 9. This language confirms that the defendant agreed to share his location with Google in order for Google to provide him with location-based services. Furthermore, the Privacy Policy provided an additional explanation to the defendant of his ability to delete his information. *Id.* at 11-12.

3. The defendant has no reasonable expectation of privacy in two hours of Google location information under the reasoning of *Carpenter*.

In *United States v. Carpenter*, 138 S. Ct. 2206, 2217 & n.3 (2018), the Supreme Court determined that individuals have a "reasonable expectation of privacy in the whole of their physical movements," and it held "that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search." The Court emphasized that its decision was "a narrow one," and it explicitly declined to determine whether there is a "limited period" for which the government can

[6] The defendant fundamentally misreads *Smith v. Maryland* when he claims that it supports his argument that courts should not consider a company's Privacy Policy in evaluating whether a customer has a reasonable expectation of privacy. *See* Def. Post-Hr'g Suppl. Br. at 27. In fact, *Smith*'s determination that users have no reasonable expectation of privacy in dialed phone numbers was based in part on Privacy Policy-like statements included in phonebooks. *See Smith*, 442 U.S. at 742-43 ("Most phone books tell subscribers, on a page entitled 'Consumer Information,' that the company 'can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.'"). In contrast, *Smith* found no Fourth Amendment significance in the phone company's interal data storage practices and definition of local-dialing zones, which do not at all resemble privacy policies. *See id.* at 745.

acquire cell phone location information without implicating the Fourth Amendment, or whether a cell tower dump constituted a search. *Id.* at 2217 n.3, 2220.

Although *Carpenter* declined to resolve whether obtaining two hours of cell phone location information constitutes a search, *Carpenter*'s reasoning suggests it does not, because *Carpenter* is focused on protecting a privacy interest in long-term, comprehensive location information. The Court began its opinion by framing the question before it as "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Carpenter*, 138 S. Ct. at 2212. The Court emphasized that long-term cell-site information created a "comprehensive record of the person's movements" that was "detailed" and "encyclopedic." *Id.* at 2216–17. It explained that "this case is not about 'using a phone' or a person's movement at a particular time." Rather, the Court explained, the case concerned "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* at 2220. By this standard, the government did not conduct a search when it obtained the two hours of the defendant's location information pursuant to the geofence warrant. Rather than providing an encyclopedic chronicle of the defendant's life, the information disclosed by Google provided a summary of his location for less than half an afternoon. This information is not quantitatively or qualitatively different from information that could be obtained from other sources, such as surveillance video or live witnesses.

In addition, in numerous cases involving other sophisticated new technologies, lower courts held that *Carpenter* protects only comprehensive, long-term location information. For example, the Seventh Circuit recently held that real-time tracking of a specified cell phone over a period of approximately six hours was not a search. *See United States v. Hammond,* — F.3d —, 2021 WL 1608789, at *7-*11 (7th Cir. Apr. 26, 2021). The Seventh Circuit previously determined

that a cell tower dump was not a search, and two other district courts reached the same result. *See United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (stating that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies))" (emphasis in original)); *United States v. Walker*, 2020 WL 4065980, at *8 (W.D.N.C. July 20, 2020) (concluding that the "privacy concerns underpinning the court's holding in *Carpenter* do not come into play" for a cell tower dump, which is limited to "particular *place* at *a limited time*") (emphasis in original)); *United State v. Rhodes*, 2021 WL 1541050, at *2 (N.D. Ga. Apr. 20, 2021) (stating that *Carpenter* "centrally relied on the strong Fourth Amendment privacy interests implicated when law enforcement monitors or obtain voluminous, detailed cell phone information of a person's physical presence compiled over a lengthy period that effectively delineates the contours of the individual's life and communications").[7] These cases all support the conclusion that the United States did not infringe the defendant's Fourth Amendment interests when it obtained two hours of his location information from Google.

Significantly, *Carpenter* did not reject the third-party doctrine or "disturb the application

[7] Similarly, courts have rejected a broad interpretation of *Carpenter* in cases involving automatic license plate reader databases, which record the time and place a license plate is observed. Obtaining a large amount of location information about an individual from such a database could potentially implicate *Carpenter*'s concerns regarding comprehensive location information. But investigators do not conduct a search when they obtain only a small quantity of location information from such a database. *See Commonwealth v. McCarthy*, 484 Mass. 493, 494 (2020) ("[W]hile the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of [automatic license plate readers], that interest is not invaded by the limited extent and use of ALPR data in this case."); *United States v. Yang*, 958 F.3d 851, 862 (9th Cir. 2020) (Bea, J., concurring) (stating that a query of a large automatic license plate recognition database that revealed only a single location point for Yang was not a search under Carpenter because "the information in the database did not reveal 'the whole of [Yang's] physical movements.'").

of *Smith* and *Miller*." *Carpenter*, 138 S. Ct. at 2220. Instead, *Carpenter* held that cell phone users do not voluntarily disclose their cell-site records to the phone company because cell-site information is collected "without any affirmative act on the part of the user beyond powering up," because "there is no way to avoid leaving behind a trail of location data," and because carrying a cell phone "is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. These factors are not present here. Google could not obtain and store the defendant's location without his undertaking multiple affirmative acts, including signing in to Google on his phone, enabling the phone's device location setting, enabling location reporting, and opting in to Location History. Gov't Ex. 3 at ¶ 10. The defendant also had discretion to delete any or all of his Location History. Gov't Ex. 3 at ¶ 15; Suppression Hr'g Tr. 321, 388, 416. And none of the services associated with Google's storage of Location History are indispensable to participation in modern society. In fact, approximately two-thirds of Google's users reject those services. Gov't Ex. 3 at ¶ 13; Suppression Hr'g Tr. 387.

Citing *Carpenter*, the defendant asserts that this Court should disregard the third-party doctrine, "Even If Mr. Chatrie Intentionally Enabled Location History." Def. Post-Hr'g Suppl. Br at 31. To do so, however, would disregard controlling precedent. *Carpenter* held based on facts specific to the cell phone provider context that Carpenter had not voluntarily disclosed his cell phone location information to the phone company, but it did not otherwise reverse or limit the third party doctrine. *See Carpenter*, 138 S. Ct. at 2220. Thus, if this Court determines that the defendant intentionally disclosed his location to Google, this Court must conclude that the defendant had no reasonable expectation of privacy in the location information the United States obtained from Google, as "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. at 743-44.

4. The defendant's remaining arguments are without merit.

None of the defendant's remaining arguments establish that the United States infringed the defendant's Fourth Amendment interest when it obtain location information from Google.

First, he argues that "Location History Is At Least As Precise as CSLI," but he fails to explain why that fact creates a reasonable expectation of privacy. Def. Post-Hr'g Suppl. Br. at 20. The third-party doctrine applies to information voluntarily disclosed to a third party; it includes no exception for accurate location information. And the Supreme Court in *Carpenter* assumed that cell-site information "is rapidly approaching GPS-level precision," *Carpenter*, 138 S. Ct. at 2219, but *Carpenter* still only protected disclosure of long-term, comprehensive location information.

Second, the defendant claims that "A Search of Location History Data Is Highly Intrusive," but this argument is neither supported by facts in the record nor sufficient to establish that he had a reasonable expectation of privacy in his location information. Def. Post-Hr'g Suppl. Br. at 21-23. As an initial matter, the principle that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" is not limited to information which is not particularly revealing about an individual. Conversations with others, dialed telephone numbers, and bank records can all contain sensitive information that an individual would like to keep private, but they are all subject to the third-party doctrine. Furthermore, the information the United States obtained from Google in this case was not particularly sensitive. Indeed, the defendant makes no claim that it revealed anything sensitive about him at all. Neither presence at a bank nor movements along public roads are particularly sensitive information. *See, e.g.*, *United States v. Knotts,* 460 U.S. 276, 285 (1983) (holding that monitoring movements along public roads using a

transponder installed in a container of chemicals was not a search).[8]

Third, the defendant cites the fact the United States obtained information about other Google users, but he provides no explanation of how this fact supports his claim that he had a reasonable expectation of privacy in the location information disclosed by Google. Def. Post-Hr'g Suppl. Br. at 22. In addition, his attempt to rely on the Fourth Amendment interests of others is foreclosed by Supreme Court precedent. The Supreme Court has squarely held that Fourth Amendment rights "may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). Defendants lack standing to challenge the government obtaining others' cell phone location information. *See, e.g.*, *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016).

Fourth, the defendant cites the fact that Google filtered through its entire Location History database to find information responsive to the warrant, Def. Post-Hr'g Suppl. Br. at 22, but he fails to explain how this filtering would give him an expectation of privacy. In determining whether a defendant has a reasonable expectation of privacy, courts consider the totality of the circumstances regarding the relationship between the defendant and the object of the search, *see United States v. Castellanos*, 716 F.3d 828, 846 (4th Cir. 2013), but they do not consider the particular legal process used by the government to obtain that object. The defendant would have had no reasonable expectation of privacy in two hours of his Google Location History regardless of whether the United States obtained it using a geofence warrant or a warrant explicitly identifying his account.

[8] The defendant's claim that "the defense was easily able to determine the likely identities of at least three individuals" from the geofence location information is not supported by the record. *See* Def. Post-Hr'g Suppl. Br. at 22. The defense's expert witness stated that he had not "figured out who anyone is." Suppression Hr'g Tr. 151. Moreover, neither identifying someone present at a bank nor identifying the neighborhood that someone visits (or even their home) is particularly invasive.

Fifth, the defendant is mistaken when he argues that "[u]nder the government's theory, people do not have an expectation of privacy in any data stored with a third-party or service provider, other than long-term CSLI." Def. Post-Hr'g Suppl. Br. at 31. Here, the defendant has no reasonable expectation of privacy in his location information because he disclosed it to Google in order for Google to provide him with location-based services. This principle does not apply in many common circumstances involving online service providers. For example, when an email service provider transmits and stores email on behalf of a customer, the email service does not typically depend on the substantive contents of the email, so the user may retain a reasonable expectation of privacy in email content information.

Finally, the defendant adopts by reference his "property-based arguments," Def. Post-Hr'g Suppl. Br. at 32, but his argument remains contrary to the fundamental principle that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443. The defendant cites no case—and the United States is aware of no case—in which a court has relied on a "property-based theory" to discard the third-party doctrine of *Smith* and *Miller* or prevent witnesses from providing evidence to the government. Justice Gorsuch's solo dissent in *Carpenter* did contemplate abandoning the third-party doctrine based on some sort of property rights theory of the Fourth Amendment, *see Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J., dissenting), but a solo dissent is not the law, and the third-party doctrine of *Smith* and *Miller* remains binding law.

B. *The Geofence Warrant Satisfied the Fourth Amendment*

The geofence warrant did not remotely resemble a general warrant. As set forth below, the warrant satisfied the Fourth Amendment because it was supported by probable cause and specified its object with particularity.

More generally, the facts of this case illustrate why use of a geofence warrant involves no unreasonable search or seizure. When law enforcement officers sought the warrant, they were investigating a serious violent crime, and they had reason to believe that the perpetrator posed a danger to the public if not identified and apprehended. Suppression Hr'g Tr. 622. The geofence warrant enabled them to solve the crime and protect the public by allowing them to obtain a limited and focused set of records from Google: location information over a two-hour interval of three identified and six unidentified individuals, and limited location information over a one-hour interval of ten other unidentified individuals.

The defendant argues that investigators should have taken a different path: "track down the owner of the car the suspect was seen in and compare that information to cell phone numbers that had connected with a nearby cell phone tower." Def. Post-Hr'g Suppl. Br. at 42. This approach would have required investigators to obtain a cell tower dump covering a much broader area, which likely would have revealed location information about thousands of people. Suppression Hr'g Tr. 55. It would have required them to obtain a list of everyone who had a blue Buick. Suppression Hr'g Tr. 578. And then it would have required them to further investigate everyone who fell within the overlap of these sets.

Although the defendant's approach would also have complied with the Fourth Amendment, it would have been substantially more intrusive than the geofence warrant, as well as being less likely to succeed and more expensive. It would be a very strange result if the Fourth Amendment were to bar use of a precise, focused investigative technique like a geofence warrant, and if it instead forced investigators to cast much broader nets. Fortunately, the defendant is mistaken, and the geofence warrant complied with the Fourth Amendment.

1. The Geofence Affidavit Established Probable Cause

Probable cause requires only "a fair probability, and not a prima facie showing, that contraband or evidence of a crime will be found in a particular place." *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (internal quotation marks omitted)). It is "not a high bar." *Id.* (quoting *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018)). In addition, this Court does not conduct *de novo* review concerning the existence of probable cause: "the duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004) (quoting *Gates*, 462 U.S. at 238–39).

Here, the affidavit in support of the geofence warrant established an ample basis for the issuing magistrate's finding of probable cause. In particular, the affidavit established: (1) that an unknown subject committed an armed bank robbery at a particular place and time; (2) that prior to the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone; (3) that the majority of cell phones were smartphones; (4) that "[n]early every" Android phone "has an associated Google account," and that Google "collects and retains location data" from such devices when the account owner enables Google location services; and (5) that Google can collect location information from non-Android smartphones if the devices are "registered to a Google account and the user has location services enabled." Gov't Ex. 2 at 6-7. From this information, there was a substantial basis for the magistrate to conclude that there was a fair probability that Google possessed evidence related to the robbery.

One United States Magistrate Judge recently explained his basis for issuing a geofence warrant in an arson investigation, including his determination that the warrant was supported by probable cause. *See In re Search Warrant Application*, 497 F. Supp. 3d 345 (N.D. Ill. 2020)

(hereinafter, "Harjani Opinion"). In that investigation, there was "no evidence in the affidavit that any of the suspects possessed cell phones." *Id.* at 355. Nevertheless, the magistrate judge noted that judges "may draw reasonable inferences about where evidence is likely to be found based on the nature of the evidence and the offense," and he determined that it was reasonable to infer that suspects and passerby witnesses would have cell phones, and that Google would have information about their location and identity. *See id.* at 355-56. He concluded that "the affidavit, when considering the totality of the circumstances and the agent's training and experience, allows the Court to conclude there is a fair probability that location data at Google will contain evidence of the arson crime, namely the identities of perpetrators and witnesses to the crime." *Id.* Here, where the robber used his phone just before the robbery, the basis for the magistrate's finding of probable cause was stronger than in the investigation addressed in the Harjani Opinion.

The probable cause determination for a geofence warrant is similar to that for a tower dump warrant, and in *United States v. James*, No. 18-cr-216, 2019 WL 325231 (D. Minn. Jan. 25, 2019), the district court held that a series of tower dump warrants satisfied the Fourth Amendment. In *James*, the government used tower dump warrants to solve a series of robberies. The defendant there argued that there was no probable cause for the warrants because it was "unknown whether a phone was used by the suspect before or after the robbery." *Id.* at *3. Nevertheless, the district court found that probable cause existed based on the affiant's representations about the "ubiquitous nature" of cell phones, the likelihood of criminals using cell phones, and the storage by cell phone companies of location information. *Id.* This reasoning similarly supports the magistrate's finding of probable cause for the geofence warrant in this case.

Two other magistrate judges from the Northern District of Illinois have written opinions denying applications for geofence warrants. The first magistrate judge found that the bounds of

the geofence sought by the government were too broad, but he stated that the government "could easily have sought a constitutionally valid search warrant" if it had "constrained the geographic size of the geofence and limited the cellular telephone numbers for which agents could seek additional information to those numbers that appear in all three defined geofences." *See In re Search of Information Stored at Premises Controlled by Google*, 2020 WL 5491763, at *7 (N.D. Ill. July 8, 2020). Whether the bounds of a particular geofence are too broad will always be based on the facts and circumstances of the investigation. In this investigation, the bounds of the geofence were appropriately drawn for the magistrate to conclude that there was a fair probability that Google possessed the specified evidence of crime. *See* Suppression Hr'g Tr. 523 (discussing the bounds of the geofence).

The second magistrate judge held that probable cause for a geofence warrant was lacking because there was not "probable cause to believe *every* person who entered the location engaged in the criminal activity." *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 752 (N.D. Ill. 2020) (emphasis in original). As the Harajani Opinoin recognized, however, "it is nearly impossible to pinpoint a search where only the perpetrator's privacy interests are impacted." Harjani Opinion, 497 F. Supp. 3d at 361-62. For example, the Fourth Amendment does not bar a search warrant to search a residence that a suspect shares with others. Both the defendant here and the second magistrate judge base their arguments on *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979), in which the Supreme Court held that the probable cause that supported a warrant to search a tavern and its bartender for drugs did not extend to a search of tavern patrons. But *Ybarra* is not a general limitation on search warrants that might reveal information concerning non-suspects; it merely held that the probable cause to search a commercial premises for drugs did not extend to a search of the businesss's patrons. The Harjani

Opinion explains why *Ybarra* does not limit a geofence warrant like the one here: "the government has established a fair probability that location data obtained will retrieve location data of perpetrators, co-conspirators and witnesses within the geofence, and the request is sufficiently particular to avoid any concerns resulting from *Ybarra*." Harjani Opinion, 497 F. Supp. 3d at 362 n.6.

The defendant makes several arguments that attempt to narrow or redefine the meaning of "probable cause." These arguments lack merit, and this Court should reject them.

First, the defendant argues that the geofence warrant lacked probable cause "because investigators admittedly had no suspects." Def. Post-Hr'g Suppl. Br. at 33. However, a search warrant need not identify specific suspects—all it must do is establish a fair probability that specified evidence will be found in the place to be searched. For example, in *Zurcher v. Stanford Daily*, 436 U.S. 547, 551 (1978), the Supreme Court approved a search warrant that authorized seizure from a newspaper of photographs of unidentified individuals who had assaulted police officers. The defendant cites no case suggesting that a warrant cannot be used to solve crime.

Second, the defendant asserts that "[p]robable cause must be based on individualized facts, not group probabilities," and he claims it was improper to infer that "the robber was a Google user or had Location History enabled." Def. Post-Hr'g Suppl. Br. at 33-34. This is error: a magistrate may "draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant." *Illinois v. Gates*, 462 U.S. 213, 240 (1983). Here, the magistrate's finding of probable cause was based on a combination of specific facts (that the bank had been robbed and that the robber carried a cell phone) and reasonable inferences (that there was a fair probability that Google stored location evidence pertaining to this crime). Warrants commonly rely on a combination of specific facts and reasonable inferences, and the defendant cites no contrary case

law. For example, in *United States v. Jones*, 942 F.3d 634, 639-40 (4th Cir. 2019), the Fourth Circuit held that a magistrate had made a reasonable inference that evidence of a defendant's threats would be found at his home. Here, the magistrate similarly made a reasonable inference that Google stored evidence of the robbery.

Third, the defendant's argument is based on an improperly constricted view of what would constitute evidence of the robbery. He focuses on whether "the robber was a Google user," Def. Post-Hr'g Suppl. Br. at 33, but the issuing magistrate here had additional reasons to believe that location information held by Google would be evidence. Investigators could use the location information directly to reconstruct what took place at the crime scene at the time of the crime. They could use it to identify any accomplices. They could use it to identify potential witnesses and obtain further evidence. They could use it to corroborate and explain other evidence, including surveillance video. They could use it to rebut potential defenses raised by the robber, including an attempt by the robber to blame someone else for his crime. Thus, although the affidavit did in fact establish a fair probability that Google would have evidence concerning the robber, the probable cause established by the warrant extended well beyond that, and it was reasonable for the magistrate to conclude that all of the information that fell within the scope of the warrant constituted evidence of crime.[9]

[9] *Messerschmidt v. Millender*, 565 U.S. 535 (2012), supports this understanding of what may constitute evidence for purposes of a search warrant. In *Messerschmidt*, police obtained a warrant for "all guns and gang-related material" in connection with a known gang member shooting at his ex-girlfriend. *Id.* at 539. In a civil suit under 42 U.S.C. § 1983, Millender challenged the warrant as overbroad, but the Supreme Court rejected the suit based on qualified immunity. *See id.* The Court provided multiple reasons why it was not unreasonable for a warrant to seek "all gang-related materials" in connection with someone shooting at his ex-girlfriend. These reasons included that it could "help to establish motive," that it could be "helpful in impeaching [the shooter]," that it could be helpful in "rebutting various defenses," and that it could "demonstrat[e] [the shooter's] connection to other evidence." *Id.* at 551-52.

2. The Geofence Warrant Was Not Overbroad and Specified its Objects with Particularity

Under the Fourth Amendment, "a valid warrant must particularly describe the place to be searched, and the persons or things to be seized." *United States v. Kimble*, 855 F.3d 604, 610 (4th Cir. 2017) (internal quotation marks omitted). In addition, the items specified to be seized pursuant to a warrant must be "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). The test "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d 743, 745 (8th Cir. 1976)). Here, the geofence warrant satisfied these requirements.

a. Overbreadth

The geofence warrant was not overbroad because it was narrowly constrained based on location, dates, and times. The warrant sought only location and identity information from Google regarding a two-hour interval for individuals present at the site of a robbery during a one-hour window. Based on the facts and circumstances investigators knew about the robbery, it was appropriately tailored toward its investigatory purpose, which was to obtain evidence to help identify and convict the armed bank robber. The geofence was based on specific features of the site of the robbery. For example, it went up to but did not cover Price Club Boulevard to the east, and it covered the area where the robber had parked. Suppression Hr'g Tr. 523. Like the geofence warrant approved in the Harjani Opinion, the government "established a fair probability that location data obtained will retrieve location data of perpetrators, co-conspirators and witnesses within the geofence." Harjani Opinion, 497 F. Supp. 3d at 362 n.6. Because the evidence the

government was authorized to obtain was "no broader than the probable cause on which it is based," the warrant was not overbroad.

The cell tower dump opinion *James* provides additional authority that the warrant here was not overbroad. In *James*, the defendant challenged the tower dump warrants used to identify him as a robber because they "allowed law enforcement to identify the location of hundreds if not thousands of cell phone users on specific days during specific time frames." *James*, 2019 WL 325231 at *3. The district court, however, found that the warrants satisfied the Fourth Amendment because they sought information that was "constrained—both geographically and temporally—to the robberies under investigation." *Id.* This reasoning is fully applicable here: the geofence warrant was appropriately constrained in space and time to obtain evidence of the robbery. Indeed, the location information obtained from Google was more narrowly constrained than the location information in James. The 150-meter radius of the geofence warrant is smaller than most cellular sites, and the government only obtained location information regarding 19 individuals, most of them never identified, rather than hundreds or thousands.[10]

The defendant argues that the geofence warrant was overbroad because Google filtered its Location History database to comply with it, but this argument is without merit. Def. Post-Hr'g Suppl. Br. at 33. He cites no case law holding that a service provider may not review a large data set in order to produce a narrowly defined set of information. Such process is not new: for example, in response to a subpoena, a phone company may review every call made by all its customers in order to find calls made to a specified phone number. *See Ameritech Corp. v.*

[10] The defendant argues that cell tower dumps are more limited than geofence warrants because cell phone companies "'index' data based on location." Def. Post-Hr'g Suppl. Br. at 35. But as discussed further below, a company's internal data structures have no Fourth Amendment significance. *See infra* pp. 36-37.

McCann, 403 F.3d 908, 910 (7th Cir. 2005).

Here, Google stores its users' location information in a single database, Sensorvault. Gov't Ex. 3 at ¶ 11. Google acesses it users' location information freely to provide them and others with location-based services. For example, Google offers its advertisers a service called "radius targeting," which requires Google to determine whether a customer is within a specified distance of a specified point. Suppression Hr'g Tr. 198. And then Google further accesses users' location information to measure store visit conversions, which it shares with the advertisers. Gov't Ex. 3 at ¶ 14; Suppression Hr'g Tr. 196-97. Here, the warrant mandated an equivalent to radius targeting, but for the purpose of solving a bank robbery, rather than selling a product. The Fourth Amendment does not prohibit Google, in response to warrant, filtering data that it accesses and uses for its own business purposes.

Moreover, Google's review of a large set of data to comply with the geofence warrant is a result of Google's internal data storage practices, not an overbroad warrant. It would be possible for Google to create an additional Location History database indexed by location. Suppression Hr'g Tr. 402-03. This database would enable Google to comply with a geofence warrant—and produce the exact same data as Google currently produces—without filtering the data of all customers. The constitutionality of a search warrant does not depend on a service provider's internal data storage practices invisible to customers and the government alike. For example, in *Smith v. Maryland*, the Supreme Court held that a phone company's internal practices regarding storage of dialed number information did not "make any constitutional difference." *Smith*, 442 U.S. at 745. This reasoning is fully applicable here to Google's choice of internal data structures. The appropriate measure for the breadth of the geofence warrant here is the data sought by the warrant, which resulted in the government obtaining location information for only 19 individuals,

all of whom were near the bank at the time of the robbery.

b. Particularity

The geofence warrant specified the items to be seized with unusual precision. The warrant authorized disclosure from Google of two hours of location information associated with electronic devices that were, within a 30 minutes on either side of a bank robbery, within 150 meters of a specified point, as well as specified subscriber information associated with those devices. Gov't Ex. 2 at 4-5. Most warrants require a human to make judgments regarding whether particular items fall within the scope of the items to be seized, but here, Google could use a computer algorithm to find the responsive information. The defendant's assertion that "[t]he items to be seized are not specified" by the geofence warrant is therefore wrong. Def. Post-Hr'g Suppl. Br. at 37.

The defendant asserts that the warrant left too much discretion to Google, but the warrant left Google no discretion at all. *See* Def. Post-Hr'g Suppl. Br. at 38. First, the defendant complains that "Google decided to search Location History data, as opposed to Web & App Activity or Google Location Services data," *see id.*, but only the Location History database held information responsive to the warrant. Gov't Ex. 3 at ¶ 20; Suppression Hr'g Tr. 211. Second, the defendant complains that Google "picked a method of calculating which devices were inside the geofence that generated a high number of false positives," Def. Post-Hr'g Suppl. Br. at 38, but the warrant itself directed Google to disclose information for devices "inside the described geographical area" during the time of the robbery. Gov't Ex. 2 at 4. Google correctly interpreted this language to mean that Google should disclose information concerning devices whose latitude and longitude coordinates fell within the circle specified by the warrant. Although there always remains a possibility of imprecision in Google's location information, and a defendant may certainly challenge at trial the weight given to this information, that possibility does not make a warrant

insufficiently particular.[11]

Nor was there anything improper about FBI TFO Hylton's correspondence with Google, in which he ultimately requested that Google produce step 2 location information about nine individuals. Suppression Hr'g Tr. 622, 642; Gov't Ex. 4 at 9. Google remains an independent actor, and courts have held that a provider like Google has a due process right to object to an order directing it to comply with a search warrant. *See, e.g.*, *In re Application*, 610 F.2d 1148, 1157 (3d Cir. 1979). Where a service provider produces a portion of the information specified by legal process, the United States does not violate the Fourth Amendment when it chooses not to litigate over the rest. A contrary rule would waste judicial resources and harm privacy. Nothing in the execution of the geofence warrant supports the defendant's argument that the warrant was insufficiently particular.

The defendant also challenges the warrant because it included the second and third steps of its three-step process, thereby allowing investigators to obtain less than the maximum quantity of location and identity information that the warrant authorized. *See* Def. Post-Hr'g Suppl. Br. at 38-39. The warrant, however, established probable cause for all the evidence that law enforcement could have obtained: identity information and two hours of location data for all individuals present

[11] The defendant exaggerates the magnitude of uncertainty associated with Google's location information. He emphasizes individual location measurements that had a large display radius. These measurements, however, were in general accompanied by other measurements for the same device with smaller display radius. For example, the defendant points to one measurment in the initial production from Google with a display radius of 387 meters. *See* Def. Post-Hr'g Suppl. Br. at 17. However, a separate measurement point for that same device taken only 23 seconds before had a display radius of only 84 meters. *See* FBI CAST Report at 22 (noting initial GeoFence returns, including for Device ID 702354289); Def. Ex. 3 (cell entries 208 and 209 for Device ID 702354289). As Special Agent D'Errico explained, Google location data of this nature (two records close in time with the same center point, but a larger second display radius) indicates that the device is traveling. Suppression Hr'g Tr. 532. The uncertainty associated with the second point does not affect the accuracy of the first.

at the site of the robbery during the hour of the robbery. The information specified by a warrant must be "no broader than the probable cause on which it is based," *Hurwitz*, 459 F.3d at 473, but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. The Harjani Opinion approved a multiple-step geofence warrant for precisely this reason: "[T]he government has established probable cause to seize all location and subscriber data within the geofence locations identified. Whether it chooses to obtain all that information, or partial information, is of no matter to the Court's consideration of the constitutionality of the warrant under the Fourth Amendment." Harjani Opinion, 497 F. Supp. 3d at 362.

The most heavily-litigated search warrant in history—the search warrant in the investigation of the Playpen child pornography website—included a similar component that allowed investigators to prioritize the evidence they seized, and courts have agreed that that component did not violate the Fourth Amendment.[12] Playpen was a dark web child pornography site with over 158,000 members. *See United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018). FBI investigators obtained a warrant authorizing a search of the computers of everyone who logged into Playpen for 30 days. *See id.* at 689. The attached affidavit, however, allowed the FBI to choose to obtain less than the maximum amount of information the warrant authorized. It explained that that "in executing the requested warrant, the FBI may deploy the NIT more

[12] Eleven Courts of Appeals have considered various challenges to the Playpen warrant, and all have ultimately rejected suppression. *See United States v. Taylor*, 935 F.3d 1279, 1281 (11th Cir. 2019) ("[W]e become today the eleventh (!) court of appeals to assess the constitutionality of the so-called 'NIT warrant.' Although the ten others haven't all employed the same analysis, they've all reached the same conclusion—namely, that evidence discovered under the NIT warrant need not be suppressed."). Approximately 100 district court cases have resolved suppression motions challenging the Playpen warrant. As discussed in Section C below, the Fourth Circuit rejected a challenge to the particularity of the Playpen warrant based on the good-faith exception. *See United States v. McLamb*, 880 F.3d 685, 689-91 (4th Cir. 2018).

discretely against particular users." *United States v. Anzalone*, 208 F. Supp. 3d 358, 363 (D. Mass. 2016).

Some defendants argued that the discretion given the FBI in executing the Playpen warrant violated the Fourth Amendment's particularity requirement, but courts uniformly rejected this argument. For example, in *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016), the court concluded that "the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site." *See also Anzalone*, 208 F. Supp. 3d at 368 ("Every court to consider this question has found the NIT search warrant sufficiently particular."). Similarly, the fact that investigators here could have and did narrow the information obtained from Google is immaterial, as the geofence warrant was based on probable cause and appropriately authorized seizure of location and identity information of anyone at the site of the robbery. Rather than violating the Fourth Amendment, the three-step process allowed investigators to further protect privacy.

Finally, even if there were a particularity problem in the three-step process for the geofence warrant, the appropriate remedy would at most be to sever the second step of the warrant and to suppress second-step information. "[E]very federal court to consider the issue has adopted the doctrine of severance, whereby valid portions of a warrant are severed from the invalid portions and only materials seized under the authority of the valid portions, or lawfully seized while executing the valid portions, are admissible." *United States v. Sells*, 463 F.3d 1148, 1154–55 (10th Cir. 2006); *see also United States v. Jones*, 2018 WL 935396, at *16–*18 (E.D. Va. Feb. 16, 2018) (discussing and applying doctrine of severance).

Here, the first step of the geofence warrant targeted narrow and clearly-defined information: anonymized location information for devices within 150 meters of the bank during

the hour of the robbery. Even if this Court were to find the second step to be constitutionally inadequate, the appropriate remedy would thus be to sever the second step and retain the first. In addition, first-step information alone was sufficient for investigators to recognize that the defendant's account likely belonged to the robber. Suppression Hr'g Tr. 549-50. Thus, even if this Court were to sever the warrant and suppress second-step information from Google, the subsequent investigation of the defendant would not be the fruit of the poisonous tree.[13]

C. *Evidence from the Geofence Warrant Should Not Be Suppressed Because Investigators Relied on it in Good Faith*

Even assuming the geofence warrant was lacking in probable cause or particularity, suppression would not be an appropriate remedy. Suppression is a remedy of "last resort," to be used for the "sole purpose" of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression "outweigh its heavy costs." *Davis v. United States*, 564 U.S. 229, 236-37 (2011). "The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144.

Search warrants for Google information about the location of its users are a new investigative technique, and there were no judicial opinions analyzing them under the Fourth Amendment when FBI TFO Hylton sought his warrant. In *United States v. McLamb*, 880 F.3d

[13] Under *Bynum*, 604 F.3d at 164, the defendant lacks a reasonable expectation of privacy in subscriber information obtained under step three of the geofence warrant, and he therefore lacks standing to challenge that portion of the warrant.

685 (4th Cir. 2018), the Fourth Circuit rejected suppression in this circumstance. The court held that when considering a motion to suppress the fruits of a novel investigative technique, suppression was inappropriate where the investigating officer consulted with counsel and then sought a warrant:

> But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what Leon's 'good faith' expects of law enforcement. We are disinclined to conclude that a warrant is 'facially deficient' where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

McLamb, 880 F.3d at 691. Here, Detective Hylton followed the approach endorsed by *McLamb*. He had consulted with prosecutors before seeking both state and federal geofence warrants. Suppression Hr'g Tr. 603-04. He had previously obtained geofence warrants from both state judges and a United States Magistrate Judge. Suppression Hr'g Tr. 603-04. No prosecutor or judge had ever found a problem with these warrants. Suppression Hr'g Tr. 604-05. In this investigation, he then sought and obtained a search warrant from a state magistrate. Detective Hylton thus did what *McLamb* calls for, and the good-faith exception precludes suppression here.

The defendant also insinuates that investigators did something wrong by using a go-by from the Computer Crime and Intellectual Property Section at the Department of Justice. Def. Post-Hr'g Suppl. Br. at 3-4. But *McLamb* affirmatively encourages such consultation: it applied the good faith exception where investigators had consulted with experts from another Department of Justice section, the Child Exploitation and Obscenity Section. *See McLamb*, 880 F.3d at 691.

The defendant notes that FBI TFO Hylton had received no training on geofence warrants, Def. Post-Hr'g Suppl. Br. at 44, but there is no indication in *McLamb* that the agents there had received training on darknet child pornography warrants. Indeed, such trainings may not exist

when a new investigative technique first arises. *McLamb* calls for direct consultation with prosecutors and then seeking a warrant, not meeting a bureaucratic training requirement. Consulting directly with experts is an effective form of training, even if it is not officially categorized as such.

Alternatively, suppression is inappropriate under the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984). When police act in "objectively reasonable reliance on a subsequently invalidated search warrant" obtained from a neutral magistrate, "the marginal or nonexistent benefits produced by suppressing evidence … cannot justify the substantial costs of exclusion." *Id.* at 922. *Leon* identified four circumstances in which an officer's reliance on a warrant would not be objectively reasonable:

> (1) when the issuing judge "was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) when "the issuing magistrate wholly abandoned his judicial role …"; (3) when "an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) when "a warrant [is] so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."

United States v. Perez, 393 F.3d 457, 461 (4th Cir. 2004) (quoting *Leon*, 468 U.S. at 923). None of these circumstances are present in this case.

The defendant argues that the good faith exception does not apply here because the affidavit was so lacking in indicia of probable cause that reliance on it was unreasonable, *see* Def. Post-Hr'g Suppl. Br. at 42-43, but he is mistaken. As an initial matter, "the threshold for establishing this exception is a high one" because "[o]fficers executing warrants are not often expected to question the conclusions of an issuing authority." *United States v. Seerden*, 916 F.3d 360, 367 (4th Cir. 2019) (quoting *Messerschmidt v. Millender*, 565 U.S. 535, 547 (2012)). The defendant claims that the warrant was based on "conjecture," Def. Post-Hr'g Suppl. Br. at 42-43, but in fact

it was based on facts and reasonable inferences from those facts. The affidavit established that the bank robber had a cell phone, that most cell phones are smartphones, and that nearly every Android phone user and some non-Android phone users use Google, and that Google may store user location information. Based on these facts, the executing officers' belief that the warrant to Google was issued based on probable cause was not entirely unreasonable, and the good-faith exception thus precludes suppression.

The defendant also argues that the good faith exception does not apply because the warrant was so facially deficient in failing to specify the things to be seized that officers could not reasonably rely on it. *See* Def. Post-Hr'g Suppl. Br. at 43. But as discussed previously, the warrant was unusually specific: Google determined the responsive information using a computer algorithm. As discussed above at pages 37-38, the warrant was limited to location information over a two-hour interval, as well as accompanying identity information, for individuals present at the site of the robbery during a one-hour interval.

The defendant further argues that the warrant left too much discretion to Google, Def. Post-Hr'g Suppl. Br. at 44, but the warrant left no discretion to Google at all. The warrant, not Google, specified the physical and temporal bounds of the geofence. The warrant authorized law enforcement, not Google, to narrow down the information to be disclosed at the warrant's second and third phase. Gov't Ex. 2 at 4. It is true that when a provider is directed to comply with a warrant, it has a due process right to challenge the warrant. *See, e.g.*, *In re Application*, 610 F.2d 1148, 1156-57 (3d Cir. 1979). But that possibility provides no evidence that the warrant was insufficiently particular.

In addition, the Fourth Circuit's decision in *McLamb* forecloses the defendant's argument that the warrant was facially deficient because its three-step process left too much discretion to

investigators. *See* Def. Post-Hr'g Suppl. Br. at 44. The defendant in *McLamb* argued to the Fourth Circuit that the Playpen warrant was insufficiently particular, in part because it allowed the FBI to "deploy the [search technique] more discretely against particular users." *See* Brief of Appellant at 46-47, *United States v. McLamb*, No. 17-4299 (available at 2017 WL 2832704). The Fourth Circuit relied on *Leon*'s good-faith exception to reject suppression, concluding that the Playpen warrant was not "so 'facially deficient ... that the executing officers [could not] reasonably presume it to be valid.'" *McLamb*, 880 F.3d at 691. Under *McLamb*, the warrant here was not facially deficient, even though it authorized investigators to obtain less evidence than they established probable cause for.

The defendant also claims that the issuing magistrate "abandoned his judicial role," but no evidence supports his claim. Def. Post-Hr'g Suppl. Br. at 41-42. The defendant begins by pointing out that the magistrate was relatively new to his job, but the defendant cites no law suggesting that *Leon* is somehow less applicable to a warrant issued by a new judge or magistrate. The defendant also notes that the magistrate spent 15 to 30 minutes reviewing the warrant application, but that was a sufficient length of time to read the relatively short affidavit and make a commonsense determination that there was a fair probability that Google possessed evidence of the bank robbery. The defendant further faults the magistrate for signing a warrant that the defendant claims lacked particularity, but as the United States has explained, the warrant specified its object with exacting particularity. *See supra* pages 37-40.

The Defendant concedes that he is "not making a *Franks* claim," but he then goes on to allege that the warrant application contained misleading information and material omissions. Def. Post-Hr'g Suppl. Br. at 45. Because he is not making a *Franks* claim, these allegations do not support an argument that the good-faith exception should not apply here. The United States notes,

however, that the defendant's allegations are incorrect. First, he claims that the information produced by Google in the first two steps was not anonymous, but in fact Google did not identify any individual until step 3, and additional research or information would have been required to identify an account owner. In the context of the language of the search warrant, that is what "anonymized information" means—the warrant stated that "anonymized information" was "a numerical identifier for the account, the type of account, time stamped location coordinates and the data source." Gov't Ex. 2 at 4. Second, the defendant faults TFO Hylton for not informing the magistrate about Google's automated data filtering processes, but TFO Hylton lacked knowledge about Google's internal data structures. Suppresion Hr'g Tr. 606-67. Third, the defendant faults FBI TFO Hylton for not addressing potential inaccuracies in Google's location information. But the fact that there is some imprecision in cell phone location measurements is common knowledge; there is no reason FBI TFO Hylton would not have expected the issuing magistrate to be aware of that fact. In sum, the affidavit contained no misleading information, and any omissions were neither material to the issuance of the warrant, nor deliberate or reckless.

Finally, there is another more general reason why the investigators' reliance on the geofence warrant was reasonable: across the country, a broad array of neutral magistrates had approved geofence warrants, thus indicating their determinations that the warrants satisfy the Fourth Amendment. Magistrate Bishop's decision to sign the warrant was no outlier: Google received approximately 9000 geofence requests in 2019. Suppression Hr'g Tr. 489. FBI TFO Hylton himself had had geofence warrants approved by two state judges and a United States Magistrate Judge. Suppression Hr'g Tr. 603-04. And no judge had written an opinion rejecting an application for a geofence warrant. Given this context, and given FBI TFO Hylton's knowledge of other judges signing geofence warrants, FBI TFO Hylton's reliance on the geofence warrant in

this investigation was reasonable.

III. CONCLUSION

For the reasons set forth in this brief, this Court should deny the defendant's motion to suppress the fruits of the GeoFence warrant.

Respectfully submitted,

RAJ PAREKH
Acting United States Attorney

By: /s/

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

REPLY TO GOVERNMENT'S RESPONSE IN OPPOSITION TO MR. CHATRIE'S MOTION FOR SUPPRESSION

Okello Chatrie, through counsel, replies as follows to the government's response to his motion to suppress evidence obtained from a "geofence" general warrant. *See* ECF No. 207-2.

I. Introduction

The Government primarily argues that nobody has an expectation of privacy in their Location History information. They do so because they cannot—and do not—contest the fact that the warrant here commanded a search of "numerous tens of millions" of people, none of whom the government had probable cause to search individually. It was astoundingly overbroad and lacking particularity.

The government tries to separate its actions from Google's by seeking refuge in a three-step process that required Google to conduct a dragnet search of Location History users. But the government developed this three-step process in partnership with Google. The government wants to reap the results of the geofence search but take no responsibility for its creation and execution. The fact is the government was responsible for every step of the search. Google never conducts searches like this for business purposes and any attempt to equate geofence warrants with Google advertising is unsupported by the facts. Google searched the accounts of tens of millions of people only because they received a warrant commanding it.

It is immaterial that Google could have structured user data to make it easier for the government to search, as the government suggests. This argument also ignores that there is at least one good reason why Google chose to organize the Sensorvault database by user account: because the data belongs to the users who created it. *See* ECF No. 59-1 at 8. Any Location History data that exists, exists only in individual accounts—it is generated by individuals; it belongs to those individuals; it is intended to be private; and so, it makes sense to store it in individual user accounts. As a result, any attempt to identify individuals in any area will necessarily entail the search of tens of millions of individual accounts.

Second, the government minimizes *United States v. Carpenter* and seeks to narrow its holding into insignificance. Instead, it relies on *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), two relics of a bygone era that the Court declined to extend in *Carpenter*. The so-called "third-party" doctrine is simply not on solid footing when it comes to digital searches and seizures, and the government's attempts to liken a geofence warrant to an "invited informant" are similarly out of touch and unpersuasive. The existence of a service agreement does not end the Fourth Amendment inquiry. On the contrary, Timothy Carpenter had an agreement with his cell phone service provider, yet the Supreme Court looked beyond that, considering context, common sense, and the sensitivity of the data, to hold that the sharing of cell phone location data was not truly "voluntary." Here, as Mr. Chatrie has demonstrated, the process of enabling Location History was also not "voluntary" in any meaningful sense.

Location History data is also far more precise than the cell tower data at issue in *Carpenter*. This precision matters because it means that Location History data is more *potent* than CSLI. A little goes a long way; it can reveal the same kind of private information with much fewer data points. A single data point from CSLI may only be capable of revealing which neighborhood or

zip code a device is in. By contrast, a single Location History data point may have GPS-level accuracy, pinpointing a device's location inside of a house or church. That is why defense expert Spencer McInvaille was able to determine the likely identities of at least three other individuals based on the supposedly "anonymized" data provided by Google during steps one and two. That is also why the government now proposes to sever the warrant; they know that even a little bit of "anonymized" data can reveal a wealth of personal information.

A geofence warrant is a digital dragnet. No matter how the government tries to dress it up or break it down, its defining features are overbreadth and lack of particularity. That is precisely why the government sought one here – they had no suspects, and they hoped a geofence search might generate one. Yet the government asks this Court to ignore the dragnet and instead rule that no one, including Mr. Chatrie, has an expectation of privacy in their Location History data. Under the government's logic, there would be no privacy right in virtually any data that involves a third-party. These arguments must be rejected. Mr. Chatrie urges this Court to find that he had an expectation of privacy in his Location History data and suppress the fruits of this modern-day general warrant.

II. Mr. Chatrie Had a Reasonable Expectation of Privacy in His Location History Data

A. The Third-Party Doctrine Does Not Apply

The government contends that the "third-party doctrine" forecloses any expectation of privacy in Location History data, *see* ECF No. 207-2 at 12, but the Supreme Court has never sanctioned a warrantless search of an individual's cell phone location data, let alone the search of millions at once. *See* 138 S. Ct. at 2219 (Court has "shown special solicitude for location information in the third-party context"). Indeed, the Court in *Carpenter* declined to extend the third-party doctrine to similar data and instructed lower courts not to "mechanically" apply old

rules to new technologies. *Id.* Yet that is precisely what the government asks this Court to do: mechanically apply precedent from the 1960s and 70s to the technology of 2021.

The government therefore invites error by likening Location History to an "invited informant," *see* ECF No. 207-2 at 12 (citing *Hoffa v. United States*, 385 U.S. 293, 302 (1966)), as if Google were no different from the guy who Jimmy Hoffa conspired with in his hotel room. The Court found it dispositive that the informant was not only in the suite by invitation, but that "every conversation which he heard was either directed to him or knowingly carried on in his presence." *Hoffa*, 385 U.S. at 302. Location History, by contrast, runs imperceptibly in the background, constantly recording, even if a user is doing nothing on the device. *See* ECF No. 205 at 26.

The government also heavily relies on *Smith v. Maryland*, 442 U.S. 735 (1979). There, the Court found no expectation of privacy in the digits dialed from a landline telephone. 442 U.S. at 742. The Court found it highly significant that callers were actively aware that they were interacting with the phone company when they placed a call, sometimes speaking with an operator, and receiving monthly bills with printouts showing the information collected. *Id.* at 742-45. In this case, by contrast, a user may enable Location History once—perhaps without even realizing it—and have no awareness that it remains on, silently recording, indefinitely. *See* ECF No. 205 at 26. Thus, if a user enabled Location History through the Google Assistant setup process, and then never used Google Assistant once, Location History would still be on and logging data every two or six minutes. *Id.* at 14, 26. Such a user would not know Location History is enabled, let alone how much data is being collected or how to manage it. Appearing to recognize that this was a problematic practice, Google eventually began sending out monthly emails to users who had enabled Location History, but Google has no record of sending such reminders to Mr. Chatrie and concedes that it may not have done so here. *See* ECF No. 205 at 30-31. Moreover, Google does

not bill users for Location History and Google does not compile Location History information for business purposes, unlike the digits dialed in *Smith*. *See* ECF No. 59-1 at 22. Consequently, Location History is not a "business record;" it is user data—content—that belongs to the individuals who created it. *See id.* at 8.

The government's reliance on *Miller* is likewise misplaced. In *Miller*, the Court found no expectation of privacy in checks, deposit slips, and statements because they were "*negotiable instruments*" intended for use in commercial transactions. 425 U.S. at 438 (emphasis added). The Court distinguished them from otherwise "confidential communications." *Id.* Location History data, by contrast, is considered "content" under the Stored Communications Act, *see* 18 U.S.C. § 2703(a) & (b), and Google treats it accordingly. *See* ECF No. 59-1 at 4. And in any event, Location History data is not a "negotiable instrument." No one gets paid in Location History. Rather, Location History is private data belonging to individual users that Google does not provide to advertisers. *See* ECF No. 205 at 9, 35; Tr. at 197 (regardless of the type of advertising, Google "never share[s] anyone's location history with a third party."); *see also Carpenter*, 138 S. Ct. at 2212 (wireless carriers "often sell aggregated location records to data brokers, without individual identifying information").

In sum, Location History is not an "invited informant." It is not a "business record." And it is not a "negotiable instrument." It is, however, significantly more revealing than the bank records in *Miller* or the telephone numbers in *Smith*. *See Carpenter*, 138 S. Ct. at 2217 ("After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."). And it is almost certainly different than whatever Lord Bacon had in mind when declaring that "all subjects … owe to the King tribute and service." ECF No. 207-2 at 13. Rather, Location History data is most like the cell site location information ("CSLI") at issue in *Carpenter*, in which the Supreme Court found the third-party doctrine inapplicable.

B. Mr. Chatrie Did Not "Voluntarily" Convey His Location Information to Google

One reason the *Carpenter* Court did not extend the third-party doctrine to CSLI was that people do not "voluntarily" convey sensitive data to the cell phone service provider in any "meaningful sense." 138 S. Ct. at 2220. Of course, cell phone users sign contracts with cell phone services providers, but the Supreme Court has never allowed such agreements to determine the contours of the Fourth Amendment. *See Smith*, 442 U.S. at 745 ("We are not inclined to make a crazy quilt of the Fourth Amendment"). Indeed, the *Carpenter* majority never mentioned the contract or terms of service.[1] Instead, the Court looked to the realities of the relationship between cell phone users and cell phone companies.

Here, the government invites this Court to simply "infer" that Google users intend to enable Location History and disclose dossiers of their every move because "Google provides services that are helpful to the user, like mapping or finding a phone," as opposed to "mere storage." ECF No. 207-2 at 14. Yet the cell phone company in *Carpenter* provided a helpful service as well. It transmitted phone calls and text messages directly to a user's mobile device, which of course required keeping track of where it was at all times. People were aware of this fact, the Court presumed. *See* 138 S. Ct. at 2211-12. Moreover, the records were "generated for commercial purposes," *id.* at 2217, and often sold in aggregate to data brokers for advertising purposes. *Id.* at 2212. Nonetheless, the Court looked to the realities of the digital age and saw that the "voluntary exposure" rationale underlying the third-party doctrine did not "hold up when it comes to CSLI" for two reasons. *Id.* at 2220.

[1] Nevertheless, it is worth reiterating that the Privacy Policies then in effect provided scant information about Location History, mentioning it just twice in two sentences. One described it only as a way to "save and manage location information in your account," while the other said "you can turn on Location History if you want traffic predictions for your daily commute." ECF No. 205 at 26-27 (quoting Def. Ex. 43 at 7-8).

First, "cell phones **and the services they provide** are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.* at 2220 (quoting *Riley*, 573 U.S. at 385) (emphasis added). There can be no serious dispute that this remains true today, although the government appears to maintain otherwise. *See* ECF No. 207-2 at 24. Their argument seems to be that some features, like Location History and "mapping," are not so indispensable. But *Carpenter* did not intend to limit Fourth Amendment protections to devices that are only capable of making calls and text messages. Instead, *Carpenter* rested on *Riley*, where the Court based its decision on the fact that modern smartphones serve many critical functions beyond making calls. *See Riley*, 573 U.S. at 393. They "are in fact minicomputers that also have the capacity to be used as a telephone." *Id.* And importantly, they "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, **maps**, or newspapers." *Id.* (emphasis added). For most users, these functions are likely to be just as essential as owning a phone in the first place. Indeed, it is difficult to imagine a consumer who would purchase a device now that was incapable of mapping or location services.

Second, the *Carpenter* Court found it significant that cell phones generate CSLI "by dint of its operation, without any affirmative act on the part of the user beyond powering up." *Id.* at 2220. Location History operates the same way once enabled, requiring no further action or interaction with the service as it quietly and constantly logs the phone's location data. As with CSLI, "[v]irtually any activity on the phone"—or no activity at all—generates Location History data, even if the user is asleep. *See* ECF No. 205 at 26; Tr. at 122 ("[T]here were no periods of data not being collected.").

The wrinkle in this case is that Location History is not absolutely required to use features like Google Maps or Google Assistant, for example. And it is technically possible to disable

Location History without disconnecting the device from the cellular network. *Cf. Carpenter*, 138 S. Ct. at 2220. At the same time, however, Google failed to inform users of these options, did not describe the full functioning of Location History, and employed a maze of location settings that made it difficult for ordinary people to understand, let alone control, the location information transmitted to Google. *See* ECF No. 205 at 23-29.

Google used an "opt-in" process that was uninformative at best, and deceptive at worst, nudging users at every turn to enable it without fully realizing what was happening. *See* ECF No. 205 at 29-31. This much is apparent from the high-profile "feedback" Google received and acknowledged from the likes of the United States Senate, the *New York Times*, and the *Associated Press*, not to mention a civil lawsuit led by the Attorney General of Arizona. *See* ECF No. 205 at 29-30. It is also apparent from Google's reforms in response to these criticisms, all of which either came too late to help Mr. Chatrie, or else didn't come at all. *See id.* at 30-31. Furthermore, it is far from clear, based on either of the two possible "consent flows" presented to Mr. Chatrie,[2] that a reasonable user would understand what Location History is, based on the partial sentence provided in the so-called "descriptive text." *See id.* at 11-12. Rather, it would be reasonable to believe that such data would be saved locally on the device itself and not with Google. *See id.* at 24. Users are neither required nor prompted to view additional "copy text" hidden behind an "expansion arrow," and they can enable Location History without ever seeing this information, which is also unilluminating. *See id.* at 13, 25.

As for disabling Location History, there is no way to turn it "off"—only to "pause" it. And even attempting to "pause" it results in an immediate, ominous pop-up warning advising users that

[2] The government maintains that there is only one possible "consent flow" in this case, *see* ECF 207-2 at 16-17, but Google testified that it could not be sure which language Mr. Chatrie would have seen (i.e., the "saves where you go" or "creates a private map" language) because it did not record the "UI" (user interface) on Mr. Chatrie's phone. *See* Tr. at 298; *see also* Def. Ex. 7 at 1-3; ECF No. 205 at 11.

doing so will result in unspecified "limited functionality" on the device. *See* ECF No. 205 at 27-28. Likewise, deleting all Location History records does not stop future collection, *see id.* at 15, and deleting the app used to enable Location History continues to allow collection. *Id.* at 14, 27. Even Google engineers found Google's location controls confusing, *see id.* at 29-30, with one employee emailing a company-wide listserv to ask: "which one of these options (some? all? none?) enter me into the wrongful-arrest lottery;" another wrote, "Add me to the list of Googlers who didn't understand how this worked." *Id.* at 30. Most recently, newly disclosed Google emails demonstrated that Google executives viewed it as a "problem" when users took advantage of easy-to-find privacy settings and then sought to obscure them in the settings menu.[3] This may well explain why Location History has been enabled by "numerous tens of millions" of Google users. It also accounts for any technical differences between Location History and CSLI when assessing whether the data is truly "shared" in a "meaningful sense." *See Carpenter*, 138 S. Ct. at 2220.

At the same time, there may be some users who affirmatively wish to keep a timeline of where they have been. And in such cases, individuals would still enjoy an expectation of privacy in their Location History data because it is their private property—data they create and save about their travels. *See* ECF No. 205 at 31-32. And because Location History tracks users all the time, it necessarily records when they are inside homes, churches, and similarly private locations, *i.e.*, constitutionally-protected spaces. Consequently, any trespass on the privacy of this digital property, especially when it reveals who or what is in a protected space, would trigger Fourth Amendment protections as well. *See* ECF No. 205 at 31-32.

[3] *See* Tyler Sonnemaker, *'Apple is eating our lunch': Google employees admit in lawsuit that the company made it nearly impossible for users to keep their location private*, Business Insider (May 28, 2021), *available at* https://www.businessinsider.com/unredacted-google-lawsuit-docs-detail-efforts-to-collect-user-location-2021-5.

The government dismisses this property-based argument as an invention of Justice Gorsuch's dissent in *Carpenter*. *See* ECF No. 207-2 at 27; ECF No. 41 at 12. But, as Mr. Chatrie has previously explained, *see* ECF No. 48 at 8-10, this understanding of the Fourth Amendment predates *United States v. Katz*, 389 U.S. 347 (1967), and has been repeatedly identified by the Supreme Court as an equally valid and independent test. *See, e.g., United States v. Jones*, 565 U.S. 400, 409 (2012) ("[A]s we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test."); *Kyllo v. United States*, 533 U.S. 27, 40 (2001) ("[W]ell into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass."); *Soldal v. Cook County*, 506 U.S. 56, 62 (1992) ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). Justice Gorsuch was merely recognizing that such an approach would have been an appropriate way to resolve *Carpenter*, had the defendant raised the argument. Mr. Carpenter did not, but Mr. Chatrie has done so consistently and adopts those arguments again. *See* ECF No. 29 at 14–16; ECF No. 48 at 8–10; ECF No. 109 at 20–21; ECF No. 205 at 32.

C. Location History Data Is Highly Sensitive and Can Be as Precise as GPS

In holding that the third-party doctrine does not apply to CSLI, the *Carpenter* Court considered not just whether people "voluntarily" share their CSLI with service providers, but also whether CSLI was different from the bank records and phone numbers in *Smith* and *Miller*. As the Court explained: "*Smith* and *Miller,* after all, did not rely solely on the act of sharing. Instead, they considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate 'expectation of privacy' concerning their contents.'" *Carpenter*, 138 S. Ct. at 2219. And in *Carpenter*, the Court recognized that there "is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id.* Unlike typical business records, CSLI "provides an intimate window into a person's life, revealing not only his particular

movements, but through them his 'familial, political, professional, religious, and sexual associations." *Id.* at 2217. Consequently, the Court determined that cell phone location records "hold for many Americans the 'privacies of life.'" *Id.* at 2217.

Location History data, no less than CSLI, provides a window into the same "privacies of life." *See* ECF No. 205 at 21-23. The government claims, however, that the data in this case was "not particularity sensitive" because "[n]either presence at a bank nor movements along public roads are particularly sensitive information." ECF No. 207-2 at 25. The government is wrong on three counts. First, the 150-meter geofence fully encompassed the Journey Christian Church, which is where Google placed Mr. Chatrie's phone most of the time. Only two of the data points from step one indicate that Mr. Chatrie was inside the bank. All the other points show him either inside the church or parked just outside of it. *See* Gov. Ex. 1 at 24. Second, because the effective range of the geofence was 387 meters, not 150 meters, the initial search encompassed not just the bank and the church, but all the private residences and businesses nearby, including a hotel. *See* ECF No. 205 at 17-18; Gov. Ex. 1 at 20. Many of these are constitutionally-protected spaces where Fourth Amendment protections are at their greatest. *See, e.g., United States v. Karo*, 468 U.S. 705, 714-15 (1984) ("Searches and seizures inside a home without a warrant are presumptively unreasonable."); *Stoner v. California*, 376 U.S. 483, 486 (1964) (requiring a warrant to search a hotel room). Additionally, the step-two data was not limited by any geofence and did in fact show people in their homes and apartments, in addition to tracking one person to a hospital. *See* ECF No. 205 at 22. Thus, as with CSLI, this kind of information "provides an intimate window into a person's life," revealing not only one's movements, but the "privacies of life" that the Court has sought to secure against "arbitrary power." *Carpenter*, 138 S. Ct. at 2214, 2217.

Third, it does not matter what data the government seized. It had no way of knowing, *ex ante*, what the geofence search would show. They cannot now justify that search based on the data they ultimately seized. But more importantly, it is a fiction that the search has a geographic limit to begin with. As Mr. Chatrie is now aware, a geofence search does not just entail searching the records of a few people in one place; it entails searching *all* Location History users in *any* place, regardless of how investigators draw the circle. *See* ECF No. 205 at 16, 33. Thus, any suggestion that a geofence search does not involve sensitive information misapprehends how it works. The government would have this Court believe that a geofence search is a garden-variety request for a few simple business records. But as in *Carpenter*, this "fails to contend with the seismic shifts in digital technology" that made the search possible in the first place. 138 S. Ct. at 2219. Consequently, the government "is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information." *Id.*

The government's remaining objection is that this case involves two hours of Location History instead of seven days of CSLI. *See* ECF No. 207-2 at 22. But two hours of Location History reveals the "privacies of life," especially when accounting for its greater precision and frequency of collection. Location History is at least as precise as CSLI, but it can also be as accurate as GPS. *See* ECF No. 205 at 20. That is because Google uses multiple data sources to estimate a user's location, including CSLI and GPS, as well as Wi-Fi and Bluetooth. *Id.* at 5. Thus, the precision varies from point to point, depending on the available inputs. *Id.* At the same time, it can do things that even GPS cannot do, like determine a user's elevation and identify the specific floor of the building they are on. Tr. at 372-73. Google also logs Location History data every two to six minutes, regardless of whether the phone is in use. *See* ECF No. 205 at 26.

By contrast, the precision of CSLI "depends on the geographic area covered by the cell site." *Carpenter*, 138 S. Ct. at 2211. This may be sufficient to place a person "within a wedge-shaped sector ranging from one-eighth to four square miles," for example. *Id.* at 2218. Or as the government demonstrated in this case, the coverage area for the three cell sites closest to the bank measures approximately 7 or 8 kilometers by 10 kilometers. Tr. at 528-29. As a result, a single CSLI data point could be used to determine which neighborhood or zip code someone was in, but it would not be accurate enough to identify the block and building. Moreover, even though cell phones 'ping' nearby cell sites several times a minute, service providers only log when the phone makes a connection, by placing a phone call or receiving a text message, for example. *See Carpenter*, 138 S. Ct. at 2211.

These differences between Location History and CSLI are significant because they affect how much data is needed to infer where someone was and what they were doing. While *Carpenter* anticipated that the precision of CSLI would improve, the Court was also faced with the fact that it was necessary to stitch together some minimum amount of CSLI to reveal the "privacies of life." The Court settled on seven days, but this was not a magic number; it was simply the number of days in the record for the shortest court order at issue. *See* 138 S. Ct. at 2266-67 (Gorsuch, J., dissenting). And in reality, that order only produced two days of CSLI. *Id.* at 2212. Moreover, *Carpenter* explicitly declined to say "whether there is any sufficiently limited period of time for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny." *Id.* at 2217 n.3.

Location History's greater precision and frequency of collection means that less time is needed to reveal the "privacies of life." It might take days of CSLI to piece together a mosaic with enough detail to be so revealing, but it takes just a little Location History to achieve the same

result. In this case, two hours was more than sufficient to identify users in sensitive and constitutionally-protected areas, including Mr. Chatrie in the church. And as Mr. Chatrie explains, the Supreme Court has repeatedly found such short-term searches to run afoul of the Fourth Amendment. *See* ECF No. 104 at 11; ECF No. 205 at 21-22 (citing *Karo*, 468 U.S. at 716, and *Kyllo*, 533 U.S. at 37). In short, *Carpenter* supports finding that Mr. Chatrie had a reasonable expectation of privacy in his Location History data.

III. The Warrant Was Overbroad

The government argues that the geofence warrant was supported by probable cause because "there was a fair probability that Google possessed evidence related to the robbery." ECF No. 207-2 at 29. And the government repeatedly refers to Google as a "witness" to the robbery. *Id.* at 1, 13. But Google neither witnessed the robbery nor independently possessed any evidence of it. Rather, people witnessed the robbery and some of those people possessed relevant Location History data in their Google accounts. The government, however, did not establish probable cause to search a single person's Google account. And they certainly did not establish probable cause to search "numerous tens of millions" of accounts.

Instead, the government engages in a Fourth Amendment slight of hand, substituting Google for the individual users they seek to search. With this trick complete, it might appear sufficient to simply recite the facts of the case, note the ubiquity of cell phones, and cite Google's popularity to establish probable cause. *See* ECF No. 207-2 at 32. But once again, Google is no "witness." Google does not own or control Location History data; users do. Google does not generate or keep Location History data; users do. It belongs to individuals, "numerous tens of millions" of them, and a geofence warrant searches every one of their accounts.[4]

[4] The government maintains that it "need not identify specific suspects," only establish that "evidence will be found in the place to be searched," ECF No. 207-2 at 32, citing *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978). But the

Because the government did not establish probable cause to search any of these accounts, they now seek to wash their hands of the massive dragnet they cast. The government does not once mention the "numerous tens of millions" of users it searched. Instead, they describe step one as "filtering" data and attribute the action to Google as if such novel searches were a routine business practice. ECF No. 207-2 at 26, 36, 46. Contrary to the government's claims, however, Google does *not* use Location History for purposes of "radius targeting." *See* ECF No. 205 at 8-9. And regardless of the advertising type, Google "never share[s] anyone's location history with a third party." *See* Tr. 197; ECF. No. 205 at 9.

The government also lays any fault for the scope of the search at Google's feet, calling it "a result of Google's internal data storage practices." *Id.* at 37. But this was no garden-variety warrant. Instead of requesting data from specific users or accounts, which Google can identify and retrieve using unique account identifiers, the government required Google to search every Location History account for relevant data. Or in other words, the government reversed the normal warrant process, searching millions before identifying any suspects or specific accounts. Once again, this is not "equivalent to radius targeting" and is not something Google ever does for purposes of "selling a product," ECF No. 207-2 at 36. It was, plain and simple, an epic dragnet compelled by the government. Location History was not designed for such purposes, *see* ECF 205 at 20, and it does not make a difference that it could have been. The government is responsible for the warrants they execute. They cannot force Google to conduct a dragnet and then disavow the consequences. The fact remains that the government did not establish probable cause to search any of the millions of accounts they Google-searched, rendering the warrant profoundly overbroad.

---

search at issue in *Zurcher* involved photographs of a demonstration taken by a newspaper employee. The newspaper owned those photographs, the photographer was a true witness to the events, and the newspaper office did not also house the private photographs taken by millions of other people. *See Zurcher*, 436 U.S. at 551.

IV. The Warrant Lacked Particularity

The government points to the geofence process as a means of redeeming an otherwise overbroad and unparticularized warrant. It says that the three-step process saves the warrant from unconstitutionality because the object of the search was clear and it was Google who "filtered" (searched) through records belonging to tens of millions of people. Yet the data to be searched and seized was the subject of significant back-and-forth between Google and the government, none of which involved a judge.

First, the search procedure was the product of repeated "engagement" between Google and the Justice Department. Tr. at 476. Google's counsel engaged with the Computer Crimes and Intellectual Property Section to discuss "certain procedures that may be relevant for the way that … Google will need to handle these types of requests, especially with reverse Location History being a relatively new type of request." Tr. at 456-57; *see also* ECF 205 at 3-4. It rings hollow, therefore, to suggest that the government was unaware of how Google would interpret the warrant, how many people would be searched in step one, or that the method used would produce a high number of false positives. The affidavit contained none of this information, however, leaving it to the government and Google to follow the procedure they created behind closed doors. Such an understanding is also evident from the plug-and-play nature of the "go by" warrant that originated with CCIPS. *See* ECF No. 205 at 4.

Second, the warrant explicitly empowered the government to determine which users to search further in steps two and three. But the particularity requirement was designed to prevent that kind of officer discretion, as two federal courts in Illinois recently determined. *See* ECF No. 205 at 38-39. In fact, there were multiple emails and phone calls between the government and Google during step two because Google did not believe it was reasonable, as the government

requested, to provide additional Location History data for all 19 users identified in step one. *See id.* at 18-19, 39. The government responds, incredibly, that they had probable cause to seize stage two *and* stage three data for all 19 of these users, meaning two hours of Location History as well as full subscriber information for each account. *See* ECF No. 207-2 at 38-39. But their reliance on the "Playpen" cases is misplaced, *see* ECF 48 at 13-14, and Mr. Chatrie maintains that the government had no probable cause for any account. Furthermore, to read the warrant in this manner would make the entire three-step process superfluous, including the requirement that the initial two rounds of data be produced in "anonymized" form. It also guts the government's argument that this process has any constitutional significance. The warrant therefore lacked particularity at each step of the way in violation of the Fourth Amendment.

V. The Good Faith Exception Does Not Apply

The government's construction of *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018) is unsupportable. There, the government received a tip about the location of computer servers hosting a message board called Playpen that allowed visitors to upload and download child pornography. *Id.* at 688. The front page of the message board displayed "two partially clothed, prepubescent girls with their legs spread apart" and was "suggestive enough that Playpen's content would be apparent to any visitor of the welcome page." *Id.* Visitors then had to enter a username and passcode to access the message board. *Id.* Playpen had about 158,000 members. *Id.* Following the tip, the government seized the Playpen servers.

Once the government seized the servers, it tried to obtain identifying information for Playpen's members, but could not because the members accessed the Playpen servers through a browser called Tor designed to conceal a user's location and activity. *Id.* To get around Tor's protections, the FBI used a digital tool that infected the Playpen servers. *Id.* Once an individual

accessed the infected Playpen server, the infected server sent instructions to the Playpen user's computer that allowed the FBI to remotely access information about the user's location and other identifying information. *Id.* at 688-89. The FBI sought a warrant allowing the FBI to install the digital tool on the Playpen servers for thirty days to identify Playpen members who entered a username and passcode within that thirty days. *Id.* at 689. The warrant accurately described the digital tool used and the scope of the intended search. *Id.* at 690.

At the time of the Playpen investigation, magistrate courts differed as to whether Federal Rule of Criminal Procedure 41 allowed a magistrate to issue a search warrant for searches that happened outside of the magistrate's district. *Id.* at 689. Concerned that its use of digital investigative tools exceeded the scope of the jurisdiction of the magistrate who authorized the Playpen search warrant, the FBI officers seeking the warrant discussed concerns about the legality of the Playpen warrant with attorneys within the Department of Justice and the FBI. *Id.* A federal magistrate in this district ultimately authorized the Playpen warrant, which allowed the FBI to use the digital tool to infect the Playpen servers and access identifying information about Playpen's members for thirty days. *Id.* Mr. McLamb was a Playpen member who accessed the Playpen servers within those thirty days. *Id.*

Mr. McLamb challenged the validity of the warrant and argued that *Leon*'s good faith exception to the Fourth Amendment did not apply. The Fourth Circuit, however, applied the good faith exception using the traditional *Leon* analysis. The court observed that there was "no indication" that the magistrate acted as a rubber stamp or that the affidavit in support of the warrant lacked a substantial basis to determine probable cause. *McLamb*, 880 F.3d at 690. It is critical to view those findings in the context of the facts of *McLamb*. First, the warrant confined the search only to members of the Playpen message board who accessed the message board within a thirty-

day timeframe. The welcome page to the message board plainly indicated to all members that entering the site provided access to child pornography, meaning that all members who accessed the site were inherently suspected of engaging in criminal activity. And second, the warrant did not give the FBI liberal discretion in executing the warrant. Those facts clearly separate the Playpen warrant from the geofence warrant in this case.

As to the first point, the warrant in this case authorized a search that is unparalleled in its overbreadth, requiring Google to search the content of accounts belonging to numerous tens of millions of people. All but a few of those individuals inherently are unconnected to the investigation in this case. All but one[5] of those individuals inherently are not suspects in this case. No search—digital or otherwise—can comply with the Fourth Amendment when it authorizes a global hunt through numerous tens of millions of innocent individuals' sensitive data.

As to the second point, the warrant in this case left immense discretion to Google and the government to execute the search. *See supra* at 16-17. This discretion was baked into the warrant, something that has troubled other courts evaluating similar geofence applications. *See, e.g.*, *Matter of Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 746 (N.D. Ill. 2020) (denying geofence warrant application, even after amendment, and observing that, unlike geofence warrant, "there was probable cause to believe [in *McLamb*] that anyone reaching the dark website was involved in possessing or trading child pornography, so that agents' discretion was in fact limited to seizing information about individuals as to whom probable cause was established"). The evidence before this Court paints the clearest picture yet as to just how much discretion the

[5] The government's assertions that a co-defendant could have been involved in the case potentially could have been a valid concern in the immediate aftermath of the robbery. But, once the police interviewed witnesses and watched the camera footage from the bank and the church—which the police did long before seeking the geofence warrant in this case, *see* Tr. at 623-25, there was no evidence to support a theory that the bank robber had co-defendants present within the geofence.

warrant left to Google and the government, which alone should preclude finding good faith.

The government very much wants to interpret *McLamb* as creating a new rule that cloaks police officers with good faith if they simply consult with an attorney before submitting a warrant. *See* ECF No. 207-2 at 41-43. *McLamb* adhered to the "traditional" *Leon* good-faith analysis. In discussing the question of the magistrate's jurisdiction to issue a warrant for a search that would inevitably search computers outside of the magistrate's district, the Fourth Circuit observed that one would expect an officer to have consulted with attorneys before seeking a search warrant that used "cutting edge investigative techniques." *McLamb*, 880 F.3d at 690-91. But *McLamb* in no way gave a "good faith" pass to police officers who consult with attorneys before submitting a warrant. Such a rule would render the qualifications in *Leon* inapplicable in every federal case, as federal prosecutors routinely review and edit federal search warrant applications. And such a rule would also do nothing to check the government overreach apparent in this case. The law enforcement community worked hand in hand with Google to develop the discretionary process set forth in the geofence warrant in this case, *see* Tr. at 455-57, 476, and further has no qualms about the unprecedented scope of the search in this case. Thus, it is up to the courts to properly apply the Fourth Amendment in this case and sanction the government overreach in this case through suppression.

VI. Conclusion

The geofence warrant in this case was devoid of probable cause and particularity, casting a digital dragnet that searched tens of millions of people. In effect, it was a general warrant, so obviously deficient that this Court should find it void and suppress all the fruits thereof.

Respectfully submitted,
OKELLO T. CHATRIE

By: /s/

Michael W. Price
NY Bar No. 4771697 (*pro hac vice*)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

/s/
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

/s/
Paul G. Gill
Va. Bar No. 31461
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0870
Fax (804) 648-5033
Paul_gill@fd.org

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA	
v.	Criminal No. 3:19CR130
OKELLO T. CHATRIE	June 24, 2021

COMPLETE TRANSCRIPT OF ARGUMENT
ON MOTION TO SUPPRESS
BEFORE THE HONORABLE M. HANNAH LAUCK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

Kenneth R. Simon, Jr., Assistant U.S. Attorney
Peter S. Duffey, Assistant U.S. Attorney
U.S. Attorney's Office
SunTrust Building
919 East Main Street, Suite 1900
Richmond, Virginia 23219

Nathan P. Judish, Assistant U.S. Attorney
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, Virginia 20530

Counsel for the United States

Laura J. Koenig, Assistant Federal Public Defender
Paul G. Gill, Assistant Federal Public Defender
Office of the Federal Public Defender
701 E. Broad Street, Suite 3600
Richmond, Virginia 23219

Counsel for the Defendant

DIANE J. DAFFRON, RPR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT

(The proceedings in this matter commenced at 10:10 a.m.)

THE CLERK: Case No. 3:19CR130, United States of America versus Okello Chatrie.

Mr. Kenneth R. Simon, Jr., Mr. Peter S. Duffey, and Mr. Nathan P. Judish represent the United States.

Mr. Paul G. Gill, Ms. Laura G. Koenig, and Mr. Michael W. Price represent the defendant.

Are counsel ready to proceed?

MR. SIMON: The United States is ready, Your Honor.

MR. GILL: The defendant is ready, Judge.

THE COURT: Well, thank you all. Obviously, we're here for argument. I want to be sure that you all know that you should proceed as you are comfortable with respect to COVID protocols. We have lifted largely most of what we're doing.

If you approach the lectern, please, I still think you should use our disinfectant in between speakers just out of safety.

All right. I'm ready to hear argument. Obviously, you have presented me with a good deal of information. So I'll hear what you have to say.

MR. PRICE: Good morning, Your Honor.

THE COURT: Good morning.

MR. PRICE: At issue in this case is a geofence warrant authorizing the search of numerous tens of millions of people without probable cause for a single one of them. It was a dragnet of epic proportions. A general warrant. The very thing the Fourth Amendment was designed to prevent.

It's obvious, or at least it should have been, that valid warrants don't look like this. There's a lot that's new about this case, but it's not new that a warrant must be supported by probable cause. It is not new that a warrant must be particularized.

So it's striking that this warrant leaves basic questions about what can be searched and seized up to Google and the government to work out, to play judge.

Good faith should therefore not apply. Valid warrants do not look like this. It was so profoundly overbroad, so lacking --

THE COURT: Sorry. I think you may have to be a little closer to the microphone. I'm sorry. Or pull it up. Yes, that's better.

MR. PRICE: I'm saying good faith should not apply. That this warrant was so overbroad, so

profoundly lacking in particularity that no reasonable officer could have relied on it.

As a result, Mr. Chatrie seeks this court to hold the warrant unconstitutional, to suppress the evidence obtained from it and all the fruits thereof.

I'd like to talk this morning first about overbreadth, then particularity, and good faith. First, I think it's very important to understand what happened here at the beginning when the initial search took place. When the government got a warrant compelling Google to search the account records of tens of millions of people. This was not something that Google normally does. It's not something that Google would have done absent the warrant. They were acting in this case as a government agent compelled by the warrant.

The search that Google did, the initial search of numerous tens of millions of people, is state action, no less than the seizure of the 19 accounts that followed or any of the steps, the warrant after that.

Google ads do not work this way. Google does not advertise and provide location information about its customers to advertisers. Google's advertising system doesn't sort through accounts in this manner.

The Sensorvault is, of course, not indexed according to location. It is indexed according to user account. And that is intentional. It's not that Google flipped a coin and decided to do it this way. It is irrelevant that they could have done it some other way. Here it is organized by user account because it is user data. It is not Google's business records.

It is not enough to simply cite statistics about Google's popularity or how many people have cell phones to establish probable cause for the kind of search that took place in this case.

There was not probable cause to search ten million user accounts. There wasn't probable cause to search 19 or 9 or even 1. There certainly wasn't probable cause to seize the account records of 19 people who happened to be nearby.

The Supreme Court has already weighed in on this, at least in the physical world. The idea that you can search people just because they are nearby to a crime was foreclosed by the Supreme Court in *Ybarro*, *Ybarro v. Illinois*. It said, "Mere propinquity is not enough. You must have probable cause with respect to each person searched and seized."

Here the government did not have probable

cause to seize all 19 accounts after the initial search.

THE COURT: Well, before you get there, I want you to explain to me how the fact that the tens of millions that were being searched were anonymized, they are not identified users, how that does or does not affect whether it's a search.

MR. PRICE: So, if you're talking about the numbers that were attached to each individual's account, those are unique identifiers that Google provided. So they're not anonymized for this time only. They are static identifiers associated with people's location history Sensorvault accounts.

So aside from the fact that it is possible to identify people based off of even a small segment of data, it would be trivial for the government in this case to obtain a subpoena, to go back to Google and to say, Okay, now please tell us the subscriber information for that anonymized number. They would not need to go back to a court to seek a warrant for that information once the Stage 1 data is turned over.

Those anonymized numbers associated with individual accounts, frankly, are not truly anonymous. It is very easy for the government to go back and get that information without a warrant just using a

subpoena for subscriber records.

THE COURT: Okay.

MR. PRICE: We would argue, Your Honor, that there was not -- we do argue that there was not probable cause to search or seize even one person's location history data in this case. There is no nexus between the robber and location history. There is some indication that the suspect had a cell phone, but there is no indication, certainly not in the warrant, that location history was enabled, something that only about a third of Google users have.

There was a -- if you take Google's view of it, there was a complex seven-step process that was required to enable it. We would say it was probably not that voluntary and knowing, but nonetheless, only a third of Google users have this enabled. So it is not enough to just say that the suspect had a cell phone. It's not clear if that suspect, that cell phone, was connected to Google. And it's not clear that that cell phone, if it was connected to Google, had location history enabled.

And, furthermore, given the uncertainty in Google's method of estimating location, there was at least another 32 percent chance that records would not be available, that somebody would be located outside

of that geofence.

So I think the percentage is certainly below 30 percent, even if you just take it by statistics. But we're saying that statistics are not enough here. There needs to be something that directly connects the warrant to the individual and the data being searched, that generalities or statistics about Google's popularity are not enough, that warrants must be -- probable cause must be individualized. And here it was not.

THE COURT: To be fair, at least some courts have relied on statistics at least to approve warrants in the past; is that right?

MR. PRICE: If you're speaking about the Illinois cases in particular, yes. One of the judges in that case looked at the statistics as an important factor in making that determination. But we argue, Your Honor, that statistics alone can never be enough, that there must be some individualized connection in each case. Otherwise, it would be simple for the government to recite those same statistics in every single case to say the facts of the crime, to say that there were cell phones involved, which is not much to accomplish these days, and that Google collects a lot of data, which is true. There would be no instance in

which the government couldn't obtain a geofence warrant.

That is why the Fourth Amendment requires that warrants be individualized, that proximate cause be individualized.

The government mentions the possibility of locating witnesses with the geofence warrant, but it is pure speculation that there were witnesses that the government had not yet identified. It seems that the most relevant witnesses the government would have already identified as being in the bank and/or through the surveillance cameras that they used initially, and that any additional witnesses found inside of buildings nearby or apartment complexes would, frankly, not have much to contribute. As one judge noted, they would have to be able to see through their walls, for starters.

The other thing I would say to that specifically is that the warrant is clearly focused on identifying a suspect, not on identifying witnesses. Witnesses are mentioned only once in passing in the context of some general information about how Google works. The clear focus of this warrant, the entire purpose of that three-step process, is designed to find the suspect, not to identify witnesses.

The same can be said of co-conspirators, which are never mentioned once in the warrant application. And, in fact, investigators knew that the suspect was seen alone coming to and from the bank based on the surveillance video.

So, once again, there are no facts to support this idea that the warrant was somehow being used for witnesses or co-conspirators in addition.

THE COURT: Well, they're saying there's not direct evidence, but they're saying because somebody was using a phone, it's likely while they were in the bank, at least there might be probable cause that they're calling a lookout.

MR. PRICE: I'm sorry?

THE COURT: That they are calling a lookout.

MR. PRICE: So, in this case, it appears that the government did an initial investigation and was aware that there wasn't another individual in the vicinity at the time. If that was the focus, it's not impossible that it --

THE COURT: So what makes you say they did the initial investigation and they knew there was not somebody there?

MR. PRICE: I believe Detective Hylton testified about the review of surveillance video they

did ahead of time, I believe it's in the CAST report as well, showing one individual leaving their car, going to the bank and back.

So if there was a concern that somebody else dropped somebody off or picked somebody up, that was already known at the time and most likely the reason the warrant is not seeking information at all about co-conspirators. They are not mentioned once.

So I think to argue that that was the point of this warrant and that there was cause for that just isn't supported on the record.

The whole point here, Your Honor, is that the government had no suspects. They were conducting a reverse warrant. They were starting with a bunch of data and trying to find a suspect based off of that. That is the reverse of how these warrants usually work when the government goes to Google and asks for information about a particular account or accounts or at least identifiable accounts. Here the whole process was turned on its head.

I'd like to shift gears to particularity, if Your Honor doesn't have any questions about overbreadth.

THE COURT: Well, I guess I want to confirm, a lot of your arguments point out that the breadth of

the search is quite overpowering and that there were other alternatives that the government could have done. Is there a legal requirement that the government use the less intrusive means to do an investigation?

MR. PRICE: No. There's no requirement that the government use the least intrusive means. I think it is different, however, to use a geofence warrant in the sense that it was more intrusive, but it is a way of trying to take a shortcut. There are, and were in this case, other avenues of investigation that the government could have pursued, traditional lines of investigation that they did not, and instead went to Google and said, "Google, tell us who robbed the bank." This was an easy way out in some sense.

THE COURT: So, Mr. Price, what I want to understand is why you're saying the shortcut is illegal. So there's no requirement for the least intrusive means. So, you know, one would hope that the government wouldn't waste resources in an investigation.

MR. PRICE: I see.

THE COURT: So what makes this illegal? It turns it on its head, but sometimes you turn something on its head and that's a good thing.

MR. PRICE: So there's nothing illegal about taking a shortcut per se, but this particular shortcut was so far afield from anything that any other court has signed off on. Certainly not the Supreme Court, not any circuit court, and there are now two different district courts, federal district courts, that have agreed that these warrants are unconstitutional. And so I think we're focusing not on the fact of a shortcut, but that this particular shortcut is completely unsupported by probable cause, and also fails the particularity requirement of the Fourth Amendment very badly at every step of the search.

Step 1, for example, goes back to this point about basic questions being left unanswered and left up to Google and the government to sort out. For example, which database to search: Location History, the Sensorvault versus Web & App Activity or Google Location Services. This was something that clearly the government had discussed with Google ahead of time, and they were both aware of which databases were going to be searched, but it wasn't in the warrant.

One reason it might not have been in the warrant is because that would require specifying that not all devices have location history enabled. So just saying we're going to search Google and Google

has location information about people makes it seem like everybody has this location information when, in fact, a third of Google users have this enabled.

So leaving out that fact wasn't a small thing. It very much dictated the overall scope of the search, which, of course, then led to tens of millions of people.

The warrant did not specify how to count if a device is inside that geofence. So we know, for example, from one of the Illinois cases, as well as the Kansas case that just came out, that the government is fully aware of this phenomenon of display radius extending beyond the geofence.

In fact, in two other cases at least, the government asked for -- explicitly told the judge that the display radius will extend beyond the geofence and that the government wants the data from everybody whose display radius even touched the geofence.

Another way to do it -- I should say that that method is likely to produce the largest number of false positives. If you are looking for anybody whose display radius intersects with that geofence in any way, there's going to be a high percentage that some of those people are going to never have been in that geofence at all. In fact, we know that happened in

this case in at least one instance where somebody was driving by and pulled in.

That's not the only way to do it. If you wanted to minimize the number of false positives, you could say, Return only the devices whose entire display radius is inside the geofence. And that would eliminate the possibility of false positives or at least drastically reduce it.

So there are multiple ways of going about this. And the government is aware of them. This warrant did not specify. And it left it up to Google and the government to sort out. The government says that Google correctly interpreted what they were intending, but none of that would be apparent to a magistrate looking at the face of this warrant.

It was likewise unclear what that geofence covers. There was no indication -- well, the government says that it was unusually specific because they identified a latitude and longitude and drew a precise circle around that, but that area is a congested urban area encompassing not just the bank, but a church and roads, at least, plus the businesses and apartments nearby that got swept in as a part of that effective range.

So we know that the effective range of the

geofence in this case was not 150 meters, that it was 387 meters, more than twice the distance of the original geofence, reaching not just that bank and the church, but Hull Street and Price Club Drive, Ruby Tuesdays, the Hampton Inn, A.M. Davis, Mini-Price Storage, the Genito Glen Apartments, and the Rockwood Village Senior Apartments. These are all places that were effectively covered by the search that the government requested here, none of which was ever signed off on by a judge or a magistrate.

The information presented to the magistrate showed a nice circle around the bank and the church and didn't mention the possibility that it would search people outside of that circle, and that the things outside of that circle that might be searched included apartment complexes, private businesses, a hotel. These are constitutionally-protected spaces. So that is significant.

And it is difficult to say that a warrant is narrowly tailored when most of the devices identified will have nothing whatsoever to do with the crime.

So even at Step 1, Your Honor, there were significant basic questions left unanswered, left to Google and the government to work out amongst themselves.

In some instances, maybe that arrangement had already been worked out, but it wasn't spelled out in the warrant. That's for sure.

Step 2 and Step 3 were far more explicit about the degree of discretion given to the government. Step 2 explicitly says that the government is going to narrow down the list and decide which people will have additional contextual location data revealed to the police. And that's the two hours total and wherever those individuals happen to go regardless of the geofence itself.

So it is at that stage completely up to the government to decide who to search, who to get more information from. Google pushed back. There was certainly a back and forth between Google here that illustrates this point very well, this negotiation between the government and Google over what is a reasonable amount of data to turn over in Stage 2.

But that is fundamentally a question that a judge should be answering, that should not be left, and cannot be left under the Fourth Amendment, up to the government to decide on its own.

Step 3 --

THE COURT: Well, before you get there, I have a question. So, with respect to Step 1 and the

identification of the 19, is there any dispute about how those 19 numbers were identified or how Google turned that information over to the government?

MR. PRICE: How it actually happened in this case?

THE COURT: Well, you're saying it got down to 19. So my question is, what is your position about how it got down to 19?

MR. PRICE: I see. So our position is that the search, the initial search, was of the numerous tens of millions of people. The 19 was the data seized from that search.

Now, there was a -- and I think is a question here that relates to particularity about how Google identified those 19 people. Google chose to say that anybody whose center points of their location -- so Google estimates location in a circle, and the latitude and longitude points are simply the center of that circle, wherever it happens to be.

The warrant in this case, the way Google interpreted it, was that anybody whose center point was inside the geofence was produced to the government as a part of that 19. I'm saying that there were other ways of going about doing that, which the government is fully aware of, and it just wasn't

spelled out one way or the other.

So one privacy protective way of doing this would be to say only return people whose display radius was entirely within the geofence. In other words, those would be much more precise readings perhaps because of GPS as opposed to Wi-Fi or cell-site location information. It would drastically reduce the number of false positives. And, as I mentioned once before, we know of one, and it's likely there are at least five in this case of those 19. So it wasn't -- this decision had consequences. And how you count who's in the circle matters.

And if it matters to determining how many sets of records you get to seize, then that's got to be something that is clear in the warrant to begin with. That can't be left up to officer discretion or Google's discretion down the road. And we make no distinction between Google and the government in this case. They are acting together, according to that warrant.

THE COURT: Is that what other courts have done?

MR. PRICE: So, the Illinois cases were decided. The opinions were issued there without the benefit of the record that we are here. And the

Kansas case, which was just decided, appears to be based on the records in the Illinois cases in terms of the factual records.

So one thing that those courts did not consider, perhaps because it wasn't known to them at the time, was the scope of this initial search that took place and how it differs, for example, from tower dumps or other types of searches.

I think had that information been known to those magistrate judges, that they would have perhaps at least paid some attention to that fact. It was just not before them. So I believe they were under the impression that Google was able to search records just in that location.

THE COURT: Well, I guess I was getting to your comment about agency. That Google and the government are -- you said Google is an agent of the government. Have other courts made that finding?

MR. PRICE: So, we do not argue that this is a private search. Google was -- which is that test for a government agent. Google was acting according to a warrant. It was compelled by legal process to assist the government; therefore, the government was not only aware of what Google was doing, but the government was directing what Google was doing.

And if Your Honor is looking for a cite on that, I would cite *Skinner v. Association of Railway Labor Executives* for the point that if you -- as the government requires, say, an employer, to conduct a drug test of their employees, that even though that's an employer, not the government, they're doing that testing at the behest of the government according to a statutory requirement, here a warrant, and therefore it is government action.

So I would say that what Google was doing here was government action. It was directed by the government.

Steps 2 and 3. Step 3, like Step 2, gave sole discretion to the government to decide which users would have their identifying information revealed. It is the same problem as in Step 2 in that the warrant explicitly gives this power to the government, which, of course, would have been obvious to the government as well as the magistrate who signed it.

There isn't a good response to that. And so the government's answer to it is that the whole three-step process doesn't matter at all, that this is just show, and they are, in fact, entitled to Stage 1, 2, and 3 data on everybody identified in that initial

geofence.

The problem with that is that it guts any argument that the three-step process has constitutional significance. And while it might take care of some of the particularity problems, it doubles the problems with probable cause. To say that no, the government actually had probable cause to search the information of all 19 people for two hours wherever they went, and to know exactly who they were, that is unsupportable from the facts. There is no allegation in the warrant or affidavit that other people that might be identified here were involved in the crime and would have evidence of criminal activity in their accounts. So it really does lay bare the probable cause problem if that's the answer to particularity.

It also would raise questions about whether a magistrate looking at this warrant would reasonably interpret that to be what it means. And so that is a relatively new argument the government has advanced, but I think if that is the route they choose to go, we would have questions about whether that's an accurate representation of what the warrant says.

Your Honor, the government also suggests that the warrant be severed and that perhaps Step 2 and Step 3 can be separated from Step 1. The problem with

severing in this case is that no part of this warrant was supported by probable cause. There is nothing to sever.

The de-anonymization doesn't matter for the reasons that I explained a little bit earlier, that it is possible to -- in fact, very trivial to identify people based off of those Sensorvault ID numbers with a mere subpoena. And that the whole process itself was nothing more than a fig leaf designed to obscure the magnitude of the search and seizure in this case.

If I can touch briefly on the question about whether this was a search. I know that that's something that the government has brought up as well. We certainly believe that *Carpenter* is the best analogy to this situation and that the Court should not try and rely on relics like *Smith* and *Miller*, outdated Supreme Court cases that are very far afield from the facts here.

Carpenter was concerned with information that reveals the privacies of life. Location history reveals the privacies of life just like CSLI and GPS. The government even got a warrant in this case, perhaps recognizing that fact. But if we want to go down that route and talk about *Carpenter*, and there are two points that the government has made for why it

doesn't fit, one that it is voluntarily conveyed to Google, and we are arguing that it is not truly voluntary, that it is not truly shared in this same sense that CSLI is not truly voluntary and shared with the company.

Here the process -- the difference being it is technically possible to turn on and off location history; however, that process of turning it on and off was highly deceptive and at the very least not meaningful or informed. But even if the Court doesn't want to go down that route, mapping and navigation apps are an essential feature of modern smartphones.

This was something that the Supreme Court recognized in *Riley* and in *Carpenter*, but when explaining the importance of cell phones to people in daily life, the Court recognized explicitly that mapping and navigation services are a part of that. And it's difficult to imagine a modern smartphone that would not provide those types of services.

Here, I think, because of the way that Google set up their opt-in process for location history, because of the way that they warned users against turning it off, saying their functionality of their phone would be degraded, that things would no longer work if they turned it off, there is a suggestion here

that this was essential to those basic features of the phone. And it would not have been apparent to users that they could turn it off and still use maps or still use Google Assistant because Google didn't tell them that. In fact, it told them the opposite. If you turn this off, bad things are going to happen to your phone.

So a reasonable user, looking at this, may not understand what they're turning on. And Google may warn them, and does warn them, against turning it off, saying that a basic function of their phone is going to be degraded if they do that. So, in that sense, we would argue that, as in *Carpenter*, this information was not voluntarily provided.

THE COURT: So, Mr. Price, I don't want to ask this question in a confusing manner, but I probably will. So, I think, for instance, this argument, you are suggesting that Google is essentially burying information about how to turn off location history and suggesting that turning off location history is problematic to the working of the phone, and at the same time you're saying only a third of folks have it turned on. So aren't those propositions contradictory?

MR. PRICE: Well, I think the ease of turning

it on might explain some of the volume there. But it's not necessary at the end of the day to find that. I think even if some -- there are going to be people in this world who actively want location history on their phone. Perhaps Mr. McGriff wants it on his phone.

I do not believe that doing so means that he has no expectation of privacy in that data, that only people that get duped into turning it on have an expectation of privacy. I think, as Google explains, this is user content. This is user property in the same way that email and photos stored with Google are user property and user content. And, therefore, searching any bit of that, even a little bit, is a search.

Google likens it to keeping a travel diary. So if you are interested in this feature, and you turn it on, Google says, Well, we're storing it in your account. Just like you might create a map with pushpins of where you've been, here's a digital equivalent that you can go back, and you can look at, and it's in your account, and it's accessible in the same way as your email, as your photos. And they treat it the same way. They treat it as user content. According to Google, it's not a business record.

What business record -- companies do not generally let customers delete their business records, yet that is something that Google permits with location history here. You can edit your location history.

THE COURT: Right. So I understand those points. So my question was the dissonance between saying both that it is not voluntary to give it over because it's so hard to turn off placed next to the fact that two-thirds of folks don't have it on, which, presumably, means they've turned it off.

MR. PRICE: Certainly some people are not enabling location history. Some people may not have occasion to or need to enable Google Assistant or may be wise at this juncture to what location history is.

I think either way you look at it, under sort of expectations of privacy test under *Carpenter* or as user data, user content that is their property, it's a search. So what I'm saying is there are two ways of getting there. And it's not necessary to find that somebody got duped in order to reach the conclusion that the Fourth Amendment protects this information.

THE COURT: Okay.

MR. PRICE: The idea that -- the other argument the government advances is that *Carpenter*

shouldn't apply because the length of time here was shorter than the seven days that the Court was talking about in *Carpenter*. I want to address that briefly, first by noting that the reason the Supreme Court chose seven days was not because it's a magic number. It was the shortest amount of time of all of the court orders for location history. So the shortest one was for seven days. That's the one the Court considered. And it is worth noting that in response to that court order, the government only actually received two days' worth of location information.

But the Court was clearly recognizing that CSLI requires some stitching together in order to paint this mosaic, to paint a picture of somebody's daily life, because any one location point from Southside location information is going to give only a fairly rough estimate of where somebody is.

The Supreme Court talks about putting somebody inside of a pie wedge that's, you know, a couple miles wide. And we would say that CSLI, at least a little bit of it, is probably enough to identify somebody's neighborhood or the ZIP code that they're in, but it is not going to be sufficient to say which house they were in.

And so the Court was looking for a way to

say, Well, how much of this do we need before it becomes a problem, before you can figure out where somebody was and what they were doing? And that's how we end up with seven days.

But the test, what they're fixated on, is what that information reveals. How much of that information do we need to get to the privacies of life? And our argument here is that geofence data is far more potent than CSLI.

Even a little bit of Google's location history data is going to be sufficient to identify somebody inside of their home or a church or another business nearby, and you don't need as much data to get the same sort of information.

I would also add that because of the precision involved here, because it does rely on GPS, and it does pinpoint people inside of their homes, as we demonstrated to the Court, that there's an additional consideration here that wasn't present in *Carpenter*, which is monitoring people inside of constitutionally-protected spaces.

The Supreme Court has been clear on this a number of times. The best examples are *Kyllo* and *Karo*, K-Y-L-L-O and K-A-R-O. In *Kyllo*, the Court looked at the use of new technology, the thermal

imager. Even though it was only trained on a house for a few moments, a couple minutes at most, law enforcement was able to determine what was happening inside that house, whether there were people inside that house. And that was enough for the Court to say it's a search. There is something special about homes under the Fourth Amendment. They are the first among equals, so to speak.

And using technology to pierce those walls and see what's going on inside and learn information you wouldn't otherwise be able to learn is a search, even if you do it for a little bit of time.

Karo was the same sort of case with an electronic beeper that had been hidden inside of a drum of chemicals inside the back of a car. That car was driven onto private property. And then the government was able to tell when that drum of chemicals was moved.

And that was, once again, information that the government would have been unable to know otherwise because it was occurring within a constitutionally-protected area that they didn't have a warrant to go and search. And the Court said you can't achieve by other means what you wouldn't be able to otherwise do, that the use of technology doesn't

give you a free pass. It, in fact, invites more scrutiny. And that's been the lesson ever sense, especially with *Jones* and *Riley* and *Carpenter*.

So I would also say that the government had to know it would get this information through either the effective range of Step 1, or, clearly, in Step 2 when people are going about their business and coming home, or going to home, and then we see that dot just sitting right on top of their house.

That was something that should have been obvious to anyone asking for this sort of warrant that even if it didn't get constitutionally-protected spaces in Stage 1, it was certainly going to get them in Stage 2. But, once again, even in Stage 1, the geofence encompasses the entirety of a church in addition to the bank. And so I don't think it's for nothing that the vast majority of data points attributed to Mr. Chatrie, all but two, from location history put him either inside the church or right next to it in a car.

And so the idea that this can't reveal information about people in constitutionally-protected spaces is false. And it should have been obvious that that was what was going to go happen to anyone who was seeking such a warrant.

THE COURT: So are you asserting at all that any of the data turned over placed Mr. Chatrie in his house?

MR. PRICE: No. We're not asserting that the data here placed Mr. Chatrie in his house, no.

THE COURT: Okay.

MR. PRICE: The government argues that this is just like the search of one place. That they name Google. They said they put down Google's corporate address, that that's one place, and it's just like searching one place. They get to search everywhere in that one place.

I think that's a sleight of hand. It ignores the mechanics of the search here. This was not like searching one house. This was like searching 10 million houses, or safe deposit boxes may be even a better example. If you want to look at what this might be like in the physical world, it would be like going to a bank and asking the bank, saying, We're looking for a weapon. We think it's in one of your safe deposit boxes. We would like you to open up every single safe deposit box in the country and look for this weapon.

That is the equivalent of what happened here. It wasn't a search of one place. It was a search of

10 million places or numerous tens of millions of places. And to try and say that this was just a search of one place at Google's headquarters is to ignore the nature of this data, to ignore that it belongs to numerous tens of millions of individuals and not to Google.

Lastly, Your Honor, I'd like to discuss good faith briefly, unless you have additional questions.

So we argue that *Leon* should not apply. That three, at least, of the exceptions that *Leon* specifically identifies apply in this case. And all three exceptions relate back to the probable cause and particularity problems that we've discussed so far, that the judge in this case, the magistrate in this case, acted -- abandoned his judicial role, acted as a rubber stamp. Looked at this warrant for 15 -- 30 minutes behind closed doors. Didn't ask a single question before signing off on it. Didn't care to ask how many people might be searched or how the government would handle the selection process in Stages 2 and 3.

This was a warrant that doesn't look like any other warrants yet the judge asked no questions. This was a warrant that explicitly gave the government the authority to decide who to search and did not ask any

questions.

These are basic questions about probable cause and particularity. But instead of addressing them as magistrate judges in Illinois and Kansas did, the judge here simply signed off and left everything up to Google and the government to work out.

The warrant was so lacking in probable cause, so overbroad, that no officer could reasonably rely on it. There wasn't probable cause to search one person's Google account. There certainly wasn't probable cause to search 19, and there was not probable cause to search tens of millions. Even if the government didn't understand that it was going to search numerous tens of millions of people, it certainly would have understood that the search they had in their mind was still going to bring in a vast majority of people who were not involved in the crime at all, for whom they had no probable cause to search and would not have been able to get a warrant to search under other circumstances.

It was only because of this fig leaf of a three-step process that made it seem like this is something that's okay. Looking at it, it is plainly -- plainly they had no suspects. They did not have probable cause to search Mr. Chatrie's account or

anyone else's. This was a fishing expedition. That should have been known to anybody looking at this warrant.

Likewise, it was so obviously deficient in particularity that it also fails under *Leon*. Giving this sort of discretion to law enforcement alone is what the particularity requirement was designed to prevent, to make sure that every petty officer didn't have the authority to go rummaging through everyone else's private papers, yet that is exactly what happened here.

No, it would not be objectively reasonable to believe that officers would have unbridled discretion to search through the location history of millions of people, especially when they didn't have any suspects.

So, Your Honor --

THE COURT: Well, let me ask you this because a not insignificant amount of your briefing suggests that this task force officer really didn't know what he was doing, didn't know that what he was asking for asked for more specific information when he got a group of 19 in the first instance, and that he should have known it was his requirement to narrow it down. So I'm trying to figure out how that feeds in to what you're saying about the discretion should not go to

the government when it appears that you're saying it's Google who's doing all this, or at least most of it, the thought processing and the narrowing down. Is that entirely dependent on your argument that Google is an agent of the government so they functionally are the government even if this task force officer really didn't understand how the process worked?

MR. PRICE: Right. So I think it's significant that the government and Google had worked out some of these details ahead of time. Even if Officer Hylton didn't know all of them personally, this was a go by.

THE COURT: When you say "Google," you're talking about the corporate level interaction with the Department of Justice? Is that what you mean?

MR. PRICE: Well, initially, it was developed between CCIPS and Google's legal team, and then here we had specific back and forth with respect to this warrant as well.

So, yes, we're saying that Google was functionally acting at the government's discretion here, that Google was compelled to act as a result of that warrant. Google was attempting to follow that warrant. That's what they were saying in response to Detective Hylton when he asked for all 19 at Stage 2

twice. And Google said, Well, we're complying with this warrant that we're legally obligated to follow, and you're not following the process.

So I think it reiterates that Google is acting in a manner that is compelled by law, that they are trying to, at least, follow the letter of that warrant, even if the government wasn't. But that, more generally, the questions that Detective Hylton maybe had about this process are attributable to the fact that this is not a normal process. This is not something they receive training on. This is not something that there are policies about. This is not something that is normally done. And so one would expect, then, there to be some confusion and questions about how it is executed.

This is a reverse warrant. This is not something like Detective Hylton or others would have normally seen or used when you're obtaining information about an individual, an individual account with a warrant that identifies that account. That is the way that this normally happens.

THE COURT: Doesn't this record show that he had done three geofence warrants before? Am I wrong about that?

MR. PRICE: I don't believe it was three

before, but --

THE COURT: I thought it was one federal and two state.

MR. PRICE: I thought it was at least one, maybe two.

THE COURT: So anyhow, he's done it before. So it's not normal, but it's not new either, right?

MR. PRICE: I suppose that is fair. It's fairly new. Even if this is only the second or third time. This is only the first time that we've actually had an opportunity to discuss this stuff in front of a judge. So all of the decisions prior to this, as Your Honor knows, were done *ex parte* based solely on the records available from this case at the time and whatever the government submitted. We still don't actually have copies of the warrants in any of those cases. They're all still under seal.

THE COURT: I just want to ask sort of random questions to make sure I don't forget them.

The United States argues that as far as the opt-in process, that this court should be bound by the testimony of Mr. McGriff because he was able to testify to the specific time frame under which Mr. Chatrie would have been using his phone, and so that your expert, who spoke about different opt-in trees,

consent flows, that I should disregard those. Are you in agreement with that?

MR. PRICE: No, Your Honor. I think Mr. McGriff was able to identify the date and time at which location history was enabled, which is only information that Google has, but Mr. McGriff was not able to say explicitly which consent flow or how it would have appeared to somebody like Mr. Chatrie. And we put forth both of those possibilities. At the time there was the "saves a private map" language and the "saves where you go with your device" language, which happened -- the change happened close in time to when location history was enabled. Mr. McGriff was unable to say exactly which one because he didn't know the operating system and software -- sorry. The operating system version that was running on Mr. Chatrie's phone.

So I think the implication there is that there's some sort of rollout process, and that it doesn't all happen literally at once like flipping a switch.

So, I guess, taking a step back from that, what I would say is that either of those two consent flows take you to the same place. That neither of them describe location history in a sufficient way to

give users informed consent over what they were agreeing to. In both instances it was less than a sentence worth of text that somebody was required to look at. And in the case of Google's Assistant, it was bundled with two other choices about enabling Voice & Audio Activity as well as device information, both of which would have been necessary to run Google Assistant, according to Google.

So, in either instance, whether you want to go with "saves a private map" or "saves where you go with this device," we do not believe that that would be sufficient to give informed consent. And we do believe that the testimony that Mr. McInvaille provided to the Court and the research that he provided or he was able to present to the Court, which the government did not contradict and Google did not contradict, I think both Google and the government were asked if they had any information to contradict Mr. McInvaille's testimony, and they said no to both.

THE COURT: All right. So, you mention a couple of times, perhaps more than that, both in argument and in briefing, that through the steps that this warrant proceeded from, Step 1 to 2, to Step 2 to 3 with no supervision, is it the case that by requiring an officer, an executing officer or law

enforcement officer, to have each return at Step 1 reviewed, and then before you go on to Step 2 or at Step 2, would that solve the constitutional concerns?

MR. PRICE: I think it might alleviate one concern with particularity. What it does not address is the Step 1 confusion, let's put it that way, about what is to be searched and seized in the first instance, which database is going to be searched, what are you counting, what area are you actually searching. All of those at Stage 1 were still left up to Google and the government to decide.

So Stage 2 and Stage 3 is more obvious because it explicitly leaves that decision up to the government. But Stage 1 is just as deficient in particularity. Even if it doesn't explicitly leave that decision up to Google and the government, it effectively did.

THE COURT: So I want to confirm, you say that the government and Google had agreed to certain parameters, for instance, searching Sensorvault. Is it the case that my record shows that the government agreed to that or that Google just did that knowing that the other repositories wouldn't have responsive information?

MR. PRICE: So I don't think we have as much

visibility as we would like into the origins of these warrants with CCIPS and Google discussing, but I don't think that ultimately matters to the outcome here.

THE COURT: So that's what I was trying to get to before. When you're saying that there's a discussion between Google and the government about what is going to be searched, i.e., Sensorvault, you're not saying that Task Force Officer Hylton had that discussion with anybody at Google. You're saying Google legal office had that conversation with CCIPS.

MR. PRICE: It appears that that's what happened. What I am saying at the end of the day is that a judge didn't say it one way or the other, which is what's required. I don't know who suggested what first, but the information was never presented in the warrant or application. It never mentions location history once, and that's a fundamental decision about what gets searched that should have been up to a judge and not some combination of Google and the government.

THE COURT: At any level, corporate level --

MR. PRICE: Correct.

THE COURT: -- or with this particular warrant.

So, with respect to the --

MR. PRICE: I was just going to go grab a

note.

THE COURT: You can go ahead. Maybe it addresses some of my questions.

MR. PRICE: First, I wanted to add to Your Honor's question about which consent flow would have been operative at the time. Mr. McGriff on pages 295 to 297 of the transcript acknowledges that he was uncertain of what language was baked in at that point in time into the phone. So that's the source of the uncertainty as to which particular language was or would have been seen.

And as we've mentioned, either way it shouldn't effect the outcome, I think, too, too much. The consent flow issue is also interesting here because we talked about what happens when you attempt to turn it off, and those sort of warnings that you get. However -- and this speaks to the voluntariness point as well -- merely turning it off does not delete the stored information that Google may have. So even if I turned off my location history right now, if I didn't actively then go and delete everything, the search would still run against me as everyone else.

Similarly, even if you delete that information, it doesn't actually turn off location history. So enabling or when Google enabled an auto

delete feature long after the facts of this case, you might be mistaken for thinking that that would have some effect on the collection of location history. In fact, it does not. And it further adds to the confusion here.

And lastly, we'd say that the consent flow isn't as probative of the expectations of privacy as the way that Google treats that data. So Google considers location history to be user content. It stores it as user content in user accounts. That's why their system is indexed this way because it belongs to the users. It is not Google's business record. And whatever weight the Court wants to put on that consent flow, it doesn't change the fact that that is individual data, the modern equivalent of their private papers stored in an individualized account.

THE COURT: All right. So my first question is, with respect to good faith, if Task Force Officer Hylton had gotten even one geofence warrant before and there is even one case that says that it's permissible, why doesn't that satisfy good faith?

MR. PRICE: There was no case saying it was permissible at the time. All of these Illinois cases came after this case. In fact, they were using some

of the early record in this case to base their decisions on. So there was no court decision on this.

In fact, I would say the -- if anything, however, the Supreme Court's focus on probable cause and particularity for the last few hundred years would signal to a reasonably well-trained officer that they need both probable cause supporting their warrant and that it must be particularized. Both of those things were glaringly absent here and that should have been apparent on its face to both Detective Hylton and to the magistrate who signed it. And the fact that Detective Hylton had done this once or twice before, I don't think changes that whatsoever. Especially, if there was no pushback or --

THE COURT: We don't know, right? All we know is that he had at least one approved, right?

MR. PRICE: We know, Your Honor, that Google, at least, reports having received quite a few of these. And it is interesting to note that this is the first case where it's actually being tested in court. Part of the reason that happens is because the geofence warrants are not always successful in identifying a suspect.

There was a different arson case being investigated in North Carolina where the geofence

warrant was reported in the news but failed to actually identify a suspect. And that could have been for any number of reasons, but one good one would be he was one of those two-thirds that did not have location history enabled.

There's a large number of these warrants that do not produce results. It is a fishing expedition. You're not always going to get a fish every time.

THE COURT: So what of the cases that we now have do you think I should look to most closely when reviewing your position?

MR. PRICE: I'm sorry? Which --

THE COURT: Which of the reported or unreported but available geofence cases that we now have is the one or two that you think I should look to most closely when reviewing this case?

MR. PRICE: I think Judge Weisman's opinion and Judge Fuentes's opinion are both very informative and well reasoned based on the facts that were available to them. I would say none of these opinions attempt to grapple with the scope of the search at Stage 1, which, simply, I don't believe was apparent at the time. But of the four that are out there now, certainly Judge Weisman and Judge Fuentes have very strong reasoned opinions when it comes to probable

cause and particularity.

THE COURT: All right.

MR. PRICE: Thank you very much, Your Honor.

THE COURT: I think those are my questions for now.

MR. PRICE: Okay. Thank you very much.

THE COURT: Okay. Thank you.

All right. So I think this is a good time to take a brief break. And we'll be back in 15 minutes, which takes us to 11:40. All right? And we'll begin with the government's position. We'll take a recess.

(Recess taken from 11:25 a.m. to 11:40 a.m.)

THE COURT: All right. I'll hear from the government.

MR. JUDISH: Thank you, Your Honor. Nathan Judish on behalf of the United States.

As we've argued consistently in this matter, there are three separate and independent reasons why this court should deny the defendant's motion to suppress.

First, that the defendant had no reasonable expectation of privacy in any of the information the government obtained from Google.

Second, that the government obtained it pursuant to a valid warrant.

And third, that investigators relied on the warrant in good faith.

I think the logical way to talk through this is to start with the question of a reasonable expectation of privacy. So I will begin with that.

I think that whether someone has a reasonable expectation of privacy turns in large part on the nature of the disclosure. And the Supreme Court has repeatedly held that one retains no reasonable expectation of privacy in information voluntarily disclosed to a third party.

And so I think it's really important to take a close look at the notion of the services Google provided here. And, essentially, Google's function here is as a location-based service provider. And so the real question is, what does a user of location-based services disclose to a location-based service provider in order to obtain location-based services? And I think the answer is pretty clear. The user discloses location information.

So consider what Google actually -- the services they -- the nature of the services they actually provide to the defendant. The main service that you disclose your location for is to get recommendations with your commute; driving

instructions and such.

So what does that mean? This isn't -- this isn't a case of someone just having Google store their location in order to create a map, although that may be one thing that they do, but you also disclose your location so Google, as a service provider, can help you get from one place to another quickly. And that involves not only Google knowing where you are and where you're going, but also Google knows where everyone else is going at the same time as well. So what you have, generally, is vast numbers of people disclosing their location to Google from which Google can assess where they are and how fast they're going and from which Google can spot traffic problems and tie-ups, one way or another, and then Google sends out advice.

You know, I'm driving down here last night on I-95 and Google says there's an accident up ahead. You can save 21 minutes by taking another route. Google doesn't know that just from my location. Google knows that from the location information it's getting from everyone.

So what we see here is that Google is using everybody's location to essentially provide useful advice to everyone. This is not people keeping their

location secret or private or anything like this. This is a big communal effort to pool location information in a way which lets Google then provide generally beneficial advice to everyone. And so it's just not kept to yourself.

And it's true that Google doesn't normally disclose any particular individual's advice [sic] to others in giving out that advice, but it's clear from controlling Supreme Court precedent in the *Miller* case that that doesn't matter. The point is, users disclose their information over to Google, and then Google, you know, is free to use that information and act on it, and so on.

THE COURT: Well, I do think you have to address the fact that, you know, *Miller*, and what we're discussing here, are facts of a different order. Right? So it is not the case, or I guess I should ask you, do you think that folks are knowingly or willingly giving over information about their location that Google updates every two minutes? I just don't think you can say that.

Most folks don't know, I think, that Google is keeping this on a two-minute loop.

MR. JUDISH: Well, as an initial matter, you can deduce just from the driving services that they're

looking at your location pretty much directly. I mean, it is really like there's something going on right now, and they act on it right now. Google has to know your information right now and act on it.

And beyond that, I mean, Google says, and it's also clear that we know from the *Smith v. Maryland* case that it doesn't matter whether you know or not that they're going to store information. The fact that you disclose it is sufficient.

So in *Smith*, you know, there was an argument that, well, customers didn't know that the phone company would actually keep records of that information, and there it didn't matter.

But, you know, as far as the -- and in addition to sort of being able to tell from using the service --

THE COURT: So I'm going to stop you there. Are you saying there is no aspect of the facts in either *Smith* or *Miller* or our case that differentiates them? The numbers we're dealing with here, if they are exponentially more than those in the other cases, that it doesn't matter?

MR. JUDISH: I mean, I don't think the frequency of storage makes much difference. I mean, you can store -- I would say, one, are users aware of

it? Well, they certainly can be because unlike with the phone company where you can't really see all the information the phone company has traditionally stored about you, your records are available to you at Google. You can log on, look at your account. You can go and see everything that they have stored. So, that's, I mean --

THE COURT: So, I'm going to say, sir, you are speaking really quickly. And I can see that my reporter is trying to keep up with you, but I can hear everything you're saying. We just have to be sure that the record follows, too.

MR. JUDISH: I will try to slow down, Your Honor.

THE COURT: Okay. Thank you.

MR. JUDISH: So, anyway, with Google you can see everything that you see stored. And so, you know, users can be aware of exactly what there is.

And, in addition, once you agree to Google saying "saves where you go with your devices," I think the frequency of it just doesn't make that much difference after that.

I mean, you can store whether it's -- you know, because people move quickly. In order for that to work well, they have to store relatively often.

And just a small, you know, small intervals, I think just don't have a great deal of significance.

So, another, I think, noteworthy aspect of how Google uses the information is in their advertising and the radius targeting that they do.

So Google, from location history, they make -- to begin with, they make certain inferences about your interests, and they target useful advertisements to you based on that. Again, that's more than just a storage service, but it goes beyond that. The radius targeting part is they will sell to customers or to advertisers the ability to place advertisements to people within a certain radius. And then in order to measure the effectiveness of that, they will subsequently examine location history information of users to see whether they have actually visited the particular store that was doing the advertising.

So that's -- I mean, that's really essentially the equivalent to a geofence because it's around the particular store that has done the advertising. So Google is doing with its own data that users provide to it, and they're quite up front about this, something which is remarkably similar to geofencing, you know, a geofence around the individual

advertiser's stores in order to, you know, provide this store visit conversion statistic to the users.

THE COURT: Yeah, but they don't identify -- I mean, they explicitly don't tell the advertisers who they are identifying.

MR. JUDISH: They don't.

THE COURT: So it's not generally the same.

MR. JUDISH: Well, again, the equivalent for the purpose of showing that the information is disclosed to Google, and it's really not necessary for the third-party doctrine for Google to, then, normally in the ordinary course of business disclose it to others. Just like a bank doesn't normally disclose your expenses to third parties outside the bank, but what you look at is what is disclosed to the party from whom the government got information.

And I think it's clear from that advertising function that you are disclosing your location information to Google.

And then that's just -- this so far has just been analyzing the nature of the service Google provides. It's also worth looking more carefully at the opt-in process and what it takes.

And as Mr. McGriff pointed out in his testimony and affidavits, it really takes a

multiple-step process before Google knows -- will ultimately store someone's location history.

So you start off with a cell phone. It's just a little electronic device sitting there. It doesn't know its location unless you first turn on the feature for your cell phone to get it to determine its location. So that's the first step you have to take.

Now the phone knows its location, but it's not telling anyone because you haven't told it to share that information with anyone. So the next step you have to take is you have to tell it to -- adjust your phone so it will share that information with apps so apps can provide you location-based services. So you do that and now the information may be shared with a Google app.

Well, okay. Google -- that's fine. Google may be able to use that location information, but it still doesn't know who you are because you haven't signed on to the Google app on your device. So that's another step you have to take before Google will end up with location information.

Okay. So you sign in on your device and now Google can determine your location.

THE COURT: Slow down.

MR. JUDISH: Slow down. This is still too

fast? All right.

So now Google can determine your location information. And it still won't store that information unless you take the additional step of opting in to location history. So all those things are affirmative steps you have to make before Google will store your location history.

And so then I want to address, because we have it in such detail, the actual opt-in process for location history. And here I think it's important -- I just want to say a bit about the record.

So, McGriff testified first through a sworn affidavit, and then he affirmed with his testimony that he stuck by his affidavits. This is from Government's Exhibit 3C at paragraph 7. Under the supported consent flow as of July 9, 2018, across all applications and services and across all Android devices and operating systems a user who opted in to LH, location history, either directly from within device settings or when attempting to use a feature powered by LH, such as features within the Google Maps application.

THE COURT: So when you read, you're even faster, which is what every human being does.

MR. JUDISH: Would be presented with an

opt-in screen containing the following text.

So McGriff said, you know, this was across all devices, across all operating systems. This was necessary opt-in language. And what he said also in his testimony was that this consent copy has been static. That's on page 271 of the transcript. He said there was possible additional descriptive copy which could change, and that, the descriptive text, he personally could not be sure about, but the actual -- this actual consent copy, he said, was static and was essential in order to opt-in. So that's why I think this court can look at the -- this consent opt-in he presented in his affidavits and be sure that that is, in fact, what he would have seen when he -- what the defendant would have seen when he opted in. And what that says is "saves where you go with your devices" and "this data may be saved and used in any Google service you are signed in to give you more personalized experiences. You can see your data, delete it, and change your settings at account.google.com."

So, I think this text really gives the core of what you're agreeing to. It says that Google's going to save where you go with your devices, and it says that Google can use that is information to

provide you with services. And that's what happens with Google's location-based services. And to that you're given a choice, either "no thanks" or "turn on," and we know because the defendant opted in on July 9, 2018, that he did, in fact, say to turn it on.

All right. So, I think all of this shows that the defendant did, in fact, voluntarily disclose his information. What does the law say here? Well, the principle that -- over and over in every single case, the Supreme Court that has addressed it, it's held that one retains no reasonable expectation of privacy in information voluntarily disclosed to third parties.

To be clear, this is not just about business records. The defendant keeps characterizing -- they're saying, well, these are not business records. I don't think it -- I mean, I think Google is clearly using the records for a business purpose, but the third party doctrine does not depend on whether or not something is a business record. It applies to conversations you do in the presence of others, for example. We know that from the *Hoffa* case.

The Supreme Court has affirmed it in multiple other contexts. We have it for everything you give to an accountant. That's the *Couch* case. We have it for

telephone dialed number information in *Smith v. Maryland*. We have it for bank records in *Miller*. And the Supreme Court has never, ever rejected that principle.

Now, *Carpenter*, the Supreme Court, obviously, did not find it applied, but the key point about *Carpenter* is that the reason it didn't apply is that the Supreme Court found that the cell-site records were not voluntarily disclosed to the phone company. And it did that for three reasons. And if you look at those three reasons, none of them apply to the location history or location information disclosed to a provider of location-based services.

First, the cell-site records are collected automatically if you just power up the device. No other affirmative action is necessary. So if you want to make phone calls, send texts, you get a cell phone. It just happens behind the scenes automatically, and there is no special opt-in process. There's certainly nothing that looks like what we have here.

The Supreme Court also noted the impossibility of deleting your cell-site records, whereas here, not only, you know, you can delete your location history stored by Google any time you want. And it's -- significantly, this fact is emphasized

over and over again by Google, even in its very minimal consent, you know, short brief text in the opt-in process. It highlights the fact you can review and delete your information at account.google.com. If you look at the Google privacy policy, it further has a long section explaining all the different ways you can delete your Google data. You know, individual data, service by service data, getting rid of your account, all that is explained at length in the Google privacy policy. So, that is not at all like cell-site records.

And, finally, the Supreme Court noted that having a cell phone was indispensable for participation in modern society. Well, I think it's quite clear that that's not the case of Google location history. Obviously, one way to establish that is empirically. We know now that only about a third of Google customers have their location history enabled. And the second way you can establish that it's not essential to participation in modern society is looking at the features associated with Google location history. They're okay. They're helpful in some circumstances, but they're just not that big a deal. The tips on your commute, finding your phone, you know, useful advertising all may be nice to some

customers, but they're not indispensable to participation in modern society.

THE COURT: Well, to be fair, you should address why Mr. Chatrie is turning to that argument. It's because Google requires a warrant under the Stored Communications Act. And so they're saying that's an indication that Google is calling it a business record. Right? Isn't that what they're saying?

MR. JUDISH: They're saying Google says it's not a business record, but I don't think whether it's a business record or not has bearing on whether it's indispensable for participation in modern society. So --

THE COURT: Yeah, but they're not arguing -- they're arguing under the Stored Communications Act that it's content. Right? That's what they are arguing.

MR. JUDISH: That's what Google is arguing. So I think whether something is classified as content under the Stored Communications Act is not that important here. It affects the rules, the statutory rules, for what kind of process the government can use to get information, but I think as a Fourth Amendment matter, it's not critical. The question is whether

Google has -- whether the records are voluntarily disclosed to Google or not.

So, and the same thing, the conversations in *Hoffa* were certainly content. That's people speaking. But because it was voluntarily disclosed to the persons who heard them, it didn't affect the -- the Fourth Amendment was not impacted when the hearer disclosed that information to the government.

So the -- whether its content has some, you know, legal significance on the kind of process you get. So I recently saw that Google had objected to a proposed state law in Texas that would allow warrants to get prospective location information from Google. They say because it's content, actually the federal law requires a wire tap order. I mean, all this is complicated statutory stuff, but not really implicated in this case. This case is about the Constitution and the Fourth Amendment, not statutory definitions or statutory rules.

I would note another point -- well, I guess, on just -- it's worth saying a little bit about *Carpenter*. *Carpenter* is, as the Supreme Court emphasized, you know, a narrow case. It's about protecting long-term comprehensive location information. The Supreme Court was clear that it said

a warrant would be required for seven days or more.

The defense here is citing *Carpenter*, essentially, for the notion that anything -- private or sensitive information requires a warrant. That is not *Carpenter*. That's not what *Carpenter* held, nor is it what any court subsequently has decided. I think, you know, *Carpenter* is no longer a totally new case. This week is its third anniversary a couple of days ago. I'm not aware of any courts who have interpreted it so broadly.

Instead, it's a uniformly -- courts have taken the Court, you know, at its word and treated it as a narrow opinion designed to protect comprehensive, long-term location information.

THE COURT: So address what they just argued. Right? They said, yes, that nobody has broadened it because we're the first folks that now know exactly what Google is doing, and we know how in depth it is, and that it covers, even if it's only a third of users, it's tens of millions. And if a court had known that, they might have come out differently.

Just agree, first of all, that other courts did not have that information.

MR. JUDISH: So, I don't think other courts had that information, other courts who have ruled thus

far. So, I think, I mean, that's very different than the *Carpenter* issue because, first, *Carpenter* is, you know -- we aren't obtaining comprehensive, long-term information about all those other people. In fact, I think it's quite doubtful that there is any Fourth Amendment significance at all for anyone whose information we did not return or who was not returned for other than the 19 people. I mean, I don't think it's a search with respect to the 19.

THE COURT: Wait. You're going way too fast. I didn't hear the last sentence at all.

MR. JUDISH: So leaving aside the 19 people, just talking about all of the others, I don't think that there's any Fourth Amendment significance at all to a provider the way a provider like Google uses automated processes to find very narrow specific information in a large database. You know, I don't think there's any significance for people whose information is not returned to the government. So --

THE COURT: Wait. Wait. I'm going to ask a question about that.

So with respect to how Google does the search, first of all, they are saying that Google is a government agent. Do you agree with that? Under the law, that they are treated as an agent.

MR. JUDISH: I don't think it's clear. When you're talking about compulsory process -- and from Google's point of view, this works an awful lot like a subpoena. And I'm not sure that someone responding, complying with compulsory process of one sort, is really quite the same as other kinds of agency relationships.

So I don't think -- I wouldn't concede that it's an agency relationship. I think things are different in terms of compulsory process. You know, when you're in litigation, and the other side receives a subpoena, are they really your agent when they're complying with a subpoena? I don't think it's clear on that. I don't think there are cases -- I'm not aware of cases that specifically address that.

THE COURT: Right. Okay. So they're saying you're not aware of it because we're the first folks that know that when the government says we want to do a geofence for this particular period of time, now we know that it's functionally Google who says, Okay, we're going to look at this area, and we're going to do it in this time frame, and it's our algorithm about how it works, and you don't get to know the algorithm. Right?

So, if you get a subpoena, it is not the

case -- well, maybe there are cases, but it's not the case that a business can say to you "I'm not going to tell you how I search for documents," right?

MR. JUDISH: Well, I mean, Google is telling -- Google's quite clear now about how they respond to the process. I mean, we give them the coordinates, and they look at each data point in their system, and they decide whether it falls within the range or not.

I mean, the part that Google is more secretive about is how they calculate the people's location in the first instance. I mean, that's the part which -- you know, so how did they come up with the particular numbers in their system for all those data things. But once they get -- they work here quite clearly, everything they did, once they got the warrant from us.

THE COURT: Well, that may be a little bit too simplistic because they said there is a range. They said that they found a range. They said there's a probabilistic return rate, like 68 percent they found appropriate for advertising, right? So I have to say, useful advertising is more a Google term than it might be a user term, but, anyhow, it's advertising. They target advertising.

So it is -- they're not saying that in a way that the government can test that it's reliable. Right? So this is what Mr. Price was just saying. He was just saying, Yeah, we don't know about the ones that haven't made hits or why because they haven't made hits.

So why is the government allowed to just say, Google, we think you're doing it right, and we'll use it when it hits? Isn't that something the government should have some input in? It's different than a subpoena.

MR. JUDISH: All of that stuff happened prior to the government getting the process in this case. Google has its own internal algorithms which they use to estimate where its users are.

THE COURT: I know, but you get the warrant knowing they have this system you don't understand, correct?

MR. JUDISH: Well, I mean, we've looked at the data that they produce, and we've seen that it's pretty accurately what --

THE COURT: It's 68 percent. Or are you saying it's better than 68 percent?

MR. JUDISH: I'm saying that it seems consistent with the notion that 68 percent of the time

the user falls within the display radius at the point that Google estimates that they are. And I believe we had testimony saying that the rest of the time it's not like it's super far off. It's often near the outside bounds of that, of the circle that Google has.

So it's not like it could be, you know, you think it's in Richmond, and you're right 68 percent of the time it's near the bank, and the other time it's, you know, across town or in another state or something like that. That's not the way it works at all.

And so what you have here, essentially, is information which is, you know, like all information, you know, it has some uncertainty in it, but it goes to -- it would ultimately go to the weight given the evidence, not the admissibility, because we've observed the information and it seems to be -- work the way Google describes it. That it --

THE COURT: Do I have any evidence about how often the geofence fails? Like how often there's just a zero hit?

MR. JUDISH: You mean, like we get a geofence and it ultimately proves unsuccessful in locating anyone or any evidence? I don't think there's anything in the record about that, Your Honor.

THE COURT: So here's the commonsensical

layperson's perspective. And so I'm really trying to give you an opportunity to explain it away. If there were drug testing that were 68 percent reliable, would it be admitted?

MR. JUDISH: I mean, I think -- I mean, I don't know about the context of drug testing, but, I mean, I think it's, you know, the definition of evidence is fairly broad. And so I would say it's evidence, but it's not all that reliable evidence, and you would hope there would be more reliable evidence.

And so, you know, in a case like this, if we go to trial, you would certainly want more than just the geofence information, and yet it's still evidence that the government collects, and then it helps direct their further investigation, which, if things go well, comes up with evidence which is even stronger and better and more probative of guilt or innocence. But it's clear that this meets the standards of what is evidence because, you know, it is helpful information which helps prove the facts which are at issue in the case.

THE COURT: Okay.

MR. JUDISH: So, a bit more -- I wanted to touch a bit more on the law associated with the third-party doctrine.

First, the defense was just -- made a point saying that sometimes you can use this information to place a person in a private space, which they suggest is a problem under *Knotts* and *Karo*, but *Knotts* and *Karo* aren't third-party doctrine cases. *Knotts* and *Karo* involve installing surreptitious transponders and tracing them. In those circumstances, we if get information from a private space without a warrant, that's a problem because it's a search.

Here, however, when we rely on the third-party doctrine, that's not an issue because the leading or a leading third-party doctrine case is the landline telephone case *Smith v. Maryland* where every time someone makes a landline call from their house, we place them in their house. And the Supreme Court says that does not matter. It's still information which is voluntarily disclosed to a third party. That issue is explicitly addressed in *Smith v. Maryland*.

Again, I just note that subsequent to *Carpenter*, the cases have all interpreted it narrowly. Within the last few weeks we had a Seventh Circuit case, *Hammond*, which held that there is no reasonable expectation of privacy in getting like six hours or so of prospective latitude-longitude-GPS-type data from an individual cell phone.

And the Court looks at *Carpenter* and says *Carpenter* is only about long-term location information. And so that *Hammond* case is three times the duration of the information at issue here. And still the Court found that the Fourth Amendment was not violated.

THE COURT: But isn't *Hammond* different in that they had a suspect in mind? What the defense is saying here is that it's a reverse search. It's like we don't know who it is.

MR. JUDISH: *Hammond* was a specific person, but as far as whether one has a reasonable expectation of privacy in the information in the first place, I just don't see -- I don't think it makes a difference. I mean, I think that it would be -- it would be -- you know, those are very different kind of warrants between a warrant for an individual's location and this type of warrant. But as far as whether one has a reasonable expectation of privacy in the information, really, I don't see how that can turn on the particular kind of legal process the government got to obtain it or didn't get to obtain it.

The question of whether there's a reasonable expectation of privacy, I think, is sort of prior to whatever kind of process the government uses to obtain

it.

One final thing on this point, just referring to *Smith* and *Miller* as relics, I mean, you know, most Supreme Court cases don't, like -- they don't, like, age out after a little while. They get reversed by the Supreme Court or they remain binding law. The Supreme Court actually affirmed them in *Carpenter* that they were still -- their continuing validity. So I just don't think you can dismiss continued binding Supreme Court precedent.

THE COURT: They're not talking necessarily about the law. They're talking about the technology involved. I mean, you have to concede this is different technology. The scope is what they're talking about, the breadth, the numbers, the detail. So, you know, in the hearing that I saw, and I think Google suggests, that if you were to go backward, as these folks are, you have -- you can make a map of where you were. You can make a little line of where you were within a period of time. And so two hours.

The question is, if you're voluntarily giving over your information, is the notice that Google is giving putting you on notice that at any two-hour period you can be mapped exactly where you are? That's their point, right? That, sure, if you're

driving down on 95, maybe intellectually you can say, Oh, you know, I have maps on. There's a tractor-trailer crash, and they're going to take me down Route 1 instead. But does that really -- does that really put a user on notice that every two hours of their life Google can track what you're doing in a comparable way? So you're saying yes.

MR. JUDISH: "Saves where you go with your devices" doesn't have qualifications with it. There are no limitations. I mean, I think, you know, that's what they do. That's what they say they'll do, and that's what they do, and that's what they show you they do if you log -- if you go where they direct and look at the data that's stored.

I just don't know. "Saves where you go with your devices" and we really mean it? I mean, I think the defense kind of explored this, and what you end up if you start trying to cover much more than that is the wall of text, which nobody would read.

THE COURT: The what? I'm sorry?

MR. JUDISH: The wall of text was the phrase that Mr. McGriff used when defense counsel suggested a rather lengthy description that they thought that Google should provide. And if they did anything like that, we'd hear, well, nobody reads that. So,

instead, what Google does is they provide a very concise description, "saves where you go with your devices," which captures what it is, and then they have an arrow, an expansion arrow, which goes into more detail, and they have a link where you can go to the website and actually see the data. I just don't -- I don't think you can do more to explain, you know, than that to effectively get across what's happening here. You tell them what you're doing and you let them see the data.

THE COURT: Well, not to mince words, but do you think it would make a difference to a user if it said "updated every two minutes"?

MR. JUDISH: No, I don't. People want the service. And if you don't do it every two minutes, it's not going to be all that effective. It's saving where you go with your device. People move quickly quite frequently and make brief stops in places, and so it wouldn't actually serve its purpose if they did much less.

THE COURT: All right.

MR. JUDISH: So, moving on to the warrant, if you don't have any more questions on the expectation of privacy.

THE COURT: If I do, I'll go back.

MR. JUDISH: All right.

So the magistrate here had a substantial basis for issuing this warrant. And the question here for this court is not would this court issue the warrant exactly like this. It's whether the magistrate had a substantial basis for issuing the warrant. And so, you know, several -- there have been in recent times several magistrate judges, federal magistrate judges, who've issued opinions on this.

They sometimes want more in the way -- they say I want more particularity in this way. This application is too broad. Those do nothing to show that there's a problem here, because, you know, the facts of those cases are different.

In one case, the geofence extends out into a denser urban area. In one case it involves a facility with several layers of apartments above it. And so getting a geofence there is just factually very easily distinguished from here.

So if you -- the question is, first, did the magistrate have a substantial basis for finding probable cause? And the question here is, was there a fair probability that Google had evidence of crime? And the facts set forth in the affidavit were sufficient to establish that.

The affidavit showed that a crime had been committed, that the robber appeared to be using a cell phone, and then established that most people have -- or that most cell phones are smartphones, that all -- nearly all Android and some Apple smartphones will be linked to Google, and that Google can store location information. That established a fair probability that Google would, in fact, have evidence of the crime.

And I think it's important to note here that evidence is not just about identifying the robber, but, you know, one of the purposes of it was to form a fuller geospatial understanding of the -- that's from page 5 -- of the warrant and timeline related to the investigation.

And so I sort of see the geofence warrant in this case as sort of similar in quality to surveillance videos. It gives you a picture of what went on at this armed bank robbery, at the time of it, sort of the people, where they were, where they're coming and going. So it's a way of going and essentially getting a new perspective on a crime scene. And it certainly does that. And so that's good evidence and, you know, a fair probability that there was evidence of a crime.

Again, it can be used to identify

accomplices. You know, it mentioned other potential witnesses, and they may not have been able to spot any other witnesses before they sought the warrant, but there could have been someone sitting in the car there back where the defendant parked. And so the notion that it was too late to -- sorry. I don't mean witness. Accomplice. That it was too late to look for other accomplices. Absolutely not. It was a totally appropriate part of this warrant to look for accomplices. It was -- that's included and is the basis for the warrant and is part of the reason why there was probable cause to get this particular warrant.

All this, the sort of a broad interpretation of what is acceptable for a search warrant, is confirmed by the Supreme Court's decision in *Messerschmit v. Millender* where they talk about sort of the broad -- sort of different reasons you might want to gather evidence, including things like (unintelligible) defenses and stuff.

THE COURT: You are really --

MR. JUDISH: I apologize for that, Your Honor.

THE COURT: I didn't hear what you said.

MR. JUDISH: So, in -- a broad conception of

evidence is confirmed by the Supreme Court's decision in -- I'll just call it *Millender* -- in which they look at a warrant and look at the reasons behind the warrant, and it's things like rebutting possible defenses. So it's a very broad conception of what constitutes evidence under a search warrant.

And this warrant sought this location information not just to identify the robber, but also for these other purposes, which are explicitly mentioned in the affidavit. So the notion of the affidavit being all about finding the robber just isn't true. You know, we don't look to, like, well, it's mostly about this other topic, and, therefore, this thing mentioned in the affidavit doesn't count. That's not the way things work.

THE COURT: So I'm just going to totally change courses so that I can have you address this on this record. And I'm going to tell you right now, I don't think it's an issue, but this is obviously a state warrant from a state magistrate. And so this magistrate was fully impowered to do what he did.

I guess I would want you to say this magistrate, who had, I don't know, a couple years experience, did not have a law degree, right? He had a college degree. And it's a pretty broad warrant.

And so my question is, do you think that the Virginia law should hold under this circumstance, right? I mean, federal magistrate judges have law degrees. And it's not clear to me that the General Assembly, when it was figuring out how magistrates work in the commonwealth of Virginia, were anticipating that they could sign warrants that searched tens of millions of user records. So I just want you to state this on the record.

MR. JUDISH: I think the magistrate was authorized under Virginia law to issue warrants, and the government doesn't always get to pick and choose. I think we have testimony in the record that there was -- the preference of the Virginia courts was to go to the magistrates rather than the state judges. So when judges -- we do what we're told, Your Honor. And this is constitutionally permissible under *Tampa v. Shadwick*, and this was a judge authorized for Virginia to issue warrants.

I still -- I still -- I disagree with the characterization of this being a search of tens of millions of people. I think the government obtained no information about those -- about anyone other than the 19.

The government can't tell, you know, if

you're not among those 19, anything about where you were that day. It doesn't know whether or not you have a Google account. What does the government know about those 19 people? It doesn't know whether you have a Google account or not. It doesn't know whether you activated location history or not. It can't tell anything about those people.

THE COURT: Why don't you distinguish the example he used about, okay, we're going into a bank. We know one of your boxes has a gun, but we want to look at them all.

MR. JUDISH: Well, I think the difference is that this is, you know, among other things, this is a database which Google has free access and free rein to, and so it's entirely appropriate in a context where Google operates freely within a database to -- for it to have Google go through and make a very -- to search through it and -- search through it not in the Fourth Amendment sense, in the computer science sense, to look through the database in order for that -- to find that narrowly targeted information.

A couple of points on this. You know, this is not an entirely new thing. I mentioned in our brief the *Ameritech v. McCann* case. I think a subpoena for the phone records of everyone in the

country would be a very troubling subpoena and overbroad under almost any circumstance you can imagine. However, for decades, you know, because phone companies store local calling information, index it only by the outgoing number and not the incoming number. When they receive a subpoena asking them who called -- you know, if they asked, like, "Who called Nathan Judish?" They have to look through their entire database and sort through that entire thing in order to get the limited information about who actually did that.

So searching through a giant database to find limited information is not a new thing. *Ameritech v. McCann* is not about a Fourth Amendment challenge. It's about who pays for that, whether the government's on the suit for the cost. No one has thought that there's a Fourth Amendment problem with looking through the huge database in order to get this very narrow targeted set of information.

Also, you know, another point that comes out of *Smith v. Maryland* is that Fourth Amendment protections really should not depend on a service provider's internal business practices which are not visible to the public.

THE COURT: Not -- I'm sorry?

MR. JUDISH: Which are not in any way visible to the public. And so in *Smith*, you know, the issue was whether it mattered that phone companies did not normally keep a record of the local phone calls that people dialed. And the Supreme Court says that doesn't matter. It has no constitutional significance. It would make a crazy quilt of the Fourth Amendment for that kind of thing to matter.

THE COURT: It would make it -- I'm sorry?

MR. JUDISH: A crazy quilt is the official term.

And so here, the fact that Google indexes its database like this is entirely invisible to the public. You know, as we've pointed out, Google could just as easily have stored this data in a different manner partitioned not by account but by location. The database would have the exact same information. It would search -- sorting through it would produce the exact same outcome from the government, and yet the Google's computers would not have to look at all the data at all. All they would have to look at is the data for whatever relevant partitions had the data for the geofence.

So the fact that this could be done without sorting through everyone's data strongly suggests that

there's no great Fourth Amendment significance to the fact that Google sorts through the data before turning over to the government only this tiny subset of the information. So, it doesn't make it a search.

I don't think I was searched by this geofence warrant. I don't think anyone whose information the government got back nothing from, I don't think the government learned anything about the rest of us. I just don't see how that's an invasion of a reasonable expectation of privacy when the government learns nothing about you. I don't think --

THE COURT: But that presumes that Google is not an agent of the government.

MR. JUDISH: I don't know if it presumes that or not. I mean, it's really -- it's -- I can't think of any case involving a search so insignificant that the Supreme Court would think of that as a search. What you learn is just so -- I don't even think you learn anything.

THE COURT: Well, they say what you learn is an anonymized number that's static that is a person or an account. And so you can readily with a subpoena find out who that is. So you're learning something, they're saying.

MR. JUDISH: We learn something about those

19 accounts. It is, to some extent, anonymized, but I'm talking about the supposed tens of millions of other searches. Those we learn nothing about. And so that's what I'm saying I just don't think that has any Fourth Amendment significance.

The defense now -- a lot of its argument is about all the people who have location history about whom the government learned nothing, not an anonymized account number, not whether they exist or not, nothing. We learned information about 19 accounts. I think it's fair to debate whether that's a search or not. But what did we learn about those supposed tens of millions? Where was the invasion of privacy when the government learned nothing? And Google learned nothing that they already didn't know. There's a giant database which they search through anyway. They didn't learn anything from it.

So, I want to go to the discretion issue associated with the warrant. The first thing I would say is this warrant just left no discretion whatsoever to Google. Google did exactly what it was directed to. The warrant directed Google to disclose location information within a particular -- of devices which were present in a specified circle of 150 meters during -- in a disclosed two hours of location

information for them during the time of the robbery.

And Google had no discretion about what database it looked through. Google should look through every database it has which contains information which is responsive to the warrant.

THE COURT: All right. So you know what? I want to be sure we're paying attention to time. When did we start? 11:40. All right. We can keep with this discretion issue, and then we'll probably take a break.

MR. JUDISH: So, Google did what they were directed to do. And everything they did is what the warrant directed. So, it isn't --

THE COURT: So, Mr. Judish, you have to address more specifically what they said. Right? So you can say Google did exactly what it was supposed to do. Right? So that's fine. But they don't say that. So you have to tell me why they're wrong.

What they say is that it just said search your databases, and somehow Google only searched Sensorvault. And there's nothing on the record that says why didn't they search Web & App Activity. Right? So they're saying somewhere there's discretion there or an agreement, but nobody knows where.

MR. JUDISH: Sorry, Your Honor. There is

stuff in the record. What's in the record is McGriff saying that the Sensorvault database is the only database which contains sufficiently granular information to be responsive to the warrant.

THE COURT: Sufficient what information?

MR. JUDISH: I don't know the exact words, but he says both in his -- that it's the only -- it's the only database with sufficiently granular information to be responsive to the warrant. So that's why they don't search the others.

As a recipient of compulsory process, they're supposed to, you know, know what they have that's responsive. As a -- someone who helps prosecute other cases, I was hoping we'd learn in this case that they had more information that they hadn't been disclosing to us that would be helpful in other investigations. Turns out, according to McGriff, they don't have that information. So what else -- if there's nothing else responsive, then they've done their job pursuant to the warrant and disclosed what they were directed to disclose.

THE COURT: So you're saying it's okay that Google knows that, but that the government doesn't know that they have only searched one?

MR. JUDISH: I'm saying that it was

appropriate for Google to do what the warrant said and give all the information they had about information which falls within the scope of the warrant. And Google -- the providers always know their databases best. And so the warrant is very specific about information it wants. And so Google, then, should look through all the information it has. And it's okay for Google to know that and not us. I mean, they don't always tell us everything --

THE COURT: So do you think that the phrase "sufficiently granular" is at all subjective?

MR. JUDISH: I mean, the -- that's McGriff's testimony. He says there aren't other databases which are responsive to the warrant.

THE COURT: Well, he says that aren't sufficiently granular. So how do we test that?

MR. JUDISH: Well, I mean, Google receives the warrant, and it complies. I mean, I think that he explained that it would be like databases which would tell you that someone is in Richmond. Obviously, a database that tells you some information that tells you someone is in Richmond isn't going to be responsive because it's not going to place someone in this circle.

And so the warrant itself is quite clear. We

want information about, you know, where you can -- about location within this circle. And so Google had, and apparently complied, with its obligation to go look at whatever data it had which could place someone within a circle like that. So --

THE COURT: And so neither the magistrate nor the agent needs to know that?

MR. JUDISH: No, I don't think so, Your Honor. We know that Google has location information. And so like Google's internal names for it and things like that, I don't think that's critical. Whatever information they had which can place someone in the geofence is going to be evidence of crime, and it's appropriate to ask them for that information.

So as far as the three-step process goes, do you want to take a break before we move on to the discretion associated with the three-step process or shall we continue?

THE COURT: You know what? I think we should take a break. So it's now twenty of one. We should take a 40-minute break so people can eat if they want to. So we'll go until 1:20. All right? We'll take a lunch recess.

(A luncheon recess is taken from 12:40 p.m. until 1:25 p.m.)

THE COURT: All right. Mr. Judish, I'm not sure if this gets to what you're going into, but I am going to just be sure that I've covered the questions that I think pertain to what you just argued.

So I spoke to you about sort of the frequency with which Google updates and stores the information, and I used two minutes. I think that's on the record, but I know that in our data return it was as quick as 30 seconds.

So in response to my question, you said, "I don't think it would matter to users if they knew it was every two minutes." So I'd like you to address the evidence that I saw and heard that Google was concerned about that. The emails that said, "Count me among the Googlers that had no idea we were doing this." And that Google actually changed its policies as far as notification because, in part, of that process, which all happened after Mr. Chatrie's case as far as I know.

MR. JUDISH: Your Honor, I think it's hard to attribute the specific changes in Google's terms and service and banners and all that to any specific thing. I mean, McGriff explained there was an ongoing process and a continued attempt to improve their process. So I just don't think you can draw any

particular inferences on any particular language from anything in the record.

I do think that it's just -- the thing to look at is -- you know, one way of looking at it is do what people do fall within the scope of the consent given by people who opted into it. You know, "saves where you go with your devices" really means saves where you go with your devices. And so whether it is, you know --

THE COURT: So it's not -- even though Google employees who work for the company that said "saves where you go with your devices" were surprised, that doesn't matter?

MR. JUDISH: I mean, there's a lot of employees who work for Google. There's a lot of people in the country, but I think the real question to look at, that we normally look at in Fourth Amendment consent situations, does this fall within the scope of the consent. And if you say "saves where you go with your devices," then you agree to that, then Google can save where you go with your devices. There is, you know, in the world of computers, lots of data gets generated in almost everything we do. To me, the unremarkable thing about this case is just how little data the government obtained.

THE COURT: You're going afar from what my question is. So you're saying that it's within the scope of the consent because this one sentence was enough, and it wouldn't have mattered if you said it is updated every two minutes because it's incorporated within that sentence, and it wouldn't have mattered as far as it being consent that it was updated every 30 seconds because it's incorporated because "Saves where you go with your devices" says "Saves where you go with your devices."

So what do I do, if anything, with the reality that no one reads that stuff? Nobody reads the privacy policy. What do I do with that?

MR. JUDISH: I mean, courts do pay attention to privacy policy (unintelligible) --

THE COURT: You definitely have to speak up. I don't know if the microphone is too far away from you or what.

MR. JUDISH: I'm sorry.

Courts certainly do pay attention to privacy policy in terms of service. The *Adkinson* case in the Seventh Circuit is an example of that. But this is more than just an obscure privacy policy thing.

The noteworthy thing about the opt-in process is how it is done through a relatively small amount of

text that Google has worked hard to get people to read. It's not long. "Saves where you go with your devices." This isn't a case where you're getting bogged down by, you know, those gigantic scroll-down-click-through things that we often have to look at.

So, I mean, I don't think it's fair to assume that people won't actually read that one little sentence before they agree to it. And, I mean, in any case, people are generally bound by their agreements, but Google really does a much better job than most other providers in getting people to agree to terms of service in trying to do this in a way that people will actually read and pay attention to.

That's one thing I took away from the McGriff testimony is they're trying hard, and they have done a pretty good job, I think. If I were to sit back and try to think what will people actually see? It's not the wall of text. It's something like what Google did here with the, like, "Saves where you go with your devices," and like one or two or three other lines for further explanation. And then if people want more, it's available. That's pretty good.

THE COURT: So tell me -- I mean, it doesn't matter whether you and I think it's good. The

question is whether or not it's constitutional and appropriately giving notice.

So where is an individual on notice about how precise the geolocation is? So one issue is if you're getting a phone number, right, you're getting a phone number. But we heard testimony that this location can be as specific as within 2 meters. So if you're getting updated every two minutes, if it's two minutes, I mean, our return had some that were 30 seconds, if you're getting updated every 30 seconds within 2 meters, are you saying that's not qualitatively different as far as a notice and an opt-in process? Where does it say we know exactly where you are?

MR. JUDISH: Well, there is mention in GPS data somewhere in all this. I'd have to look to see where it is. But people know that GPS is accurate to within a few meters. And there's mention of Wi-Fi. I don't know if it's as readily known, but people who know anything about this know that Wi-Fi is accurate, but not as accurate as GPS, but it's still reasonably accurate. And also it says because -- and this is, again, quite remarkable. Google says from the little opt-in screen "You can review your data" and it gives you a link. And you can go and you can actually see

the data. So that's distinguishes it from the information stored by phone companies. And even in the *Smith* days, you didn't know what data you had. Here you really can. Google will tell you every bit of data it stores about you. You can download it all in one piece if you want and take a look at it or you can look at it online. So Google's not hiding the ball.

THE COURT: So most of the GPS cases that I am aware of that say it's constitutional involve instances where folks are being followed on public roads. So I think what the defense is saying here is that one of the issues is that this GPS data, or whatever it is, within 2 meters can include constitutionally protected spaces like a church. So that's what I have in front of me.

They're not claiming that we found Mr. Chatrie in his house. But they're saying he was in a church. You can't do that.

MR. JUDISH: Again, Your Honor, I think I covered this point before, but *Knotts* and *Karo* are about surreptitious tracking. They're not about information disclosed to a third party.

In *Smith v. Maryland*, that involved a landline telephone. There were people sitting in

their house making phone calls. You can place a person, in those days, on a call on a landline phone also within a few meters, because how long were the phone cords? Not that long, typically. But in any case, they certainly placed people within a private space. And the Supreme Court said it didn't matter, that you could determine people were in their home within a private space because the person was disclosing the information to a third party.

And here people are choosing to disclose their information to Google in order for Google to provide them with location-based services. So it doesn't violate the Fourth Amendment when Google then shares that information with the government.

THE COURT: So if you're making a phone call out of your house, you're in a private space. So I guess if you make five phone calls in one day, the government is aware you're in your house five times in one day or at least a phone number is being dialed out in one day. But with respect to most of the tower dump cases, right, isn't it the case that it's not seeking a single data point, right? It's like watching a phone go down a street. Am I right about that? So you're going to different towers?

MR. JUDISH: Most of the published cases have

involved searching multiple towers. Certainly not all tower dump cases are like that. Sometimes we're just interested in dumps at a particular place and a particular time.

Mostly that's going to be useful if there's, you know, a place where there's not a lot of people. I remember one case that I consulted on, someone had dumped a body in an obscure location sometime between midnight and 6:00 a.m. In that case, a single place tower dump would be helpful.

THE COURT: Right. So when you get a tower dump, is it the case -- and I guess I want you to compare what's happening in this with us here.

So I think what you're saying is Google looks at not tens of millions, but lots of records that the government doesn't really see. Do they disclose the bigger amount?

MR. JUDISH: No, Your Honor, not at all.

THE COURT: Stage I is not disclosed at all?

MR. JUDISH: Stage 1, we get information about the 19 individuals who had data points present in the geofence during the hour of the bank robbery. That's it. They don't give us any information about tens of millions. We don't know how many people there are. We don't know how many people have location

history enabled or anything like that. All we get information on is 19 people. There's nothing beyond that.

THE COURT: So if you're getting a tower dump, when you're dumping the towers, are you getting just the 19 people three times or are you getting everything on the tower? Is the government doing the comparing?

MR. JUDISH: The government does the comparing on tower dumps. So typical tower dumps often involve hundreds of thousands of records. So that's why, as we explained in our briefs, this process -- the geofence warrants tend to be much more limited than a tower dump because in tower dumps, we actually learn information about a lot more people being in the vicinity for each tower dump we get.

THE COURT: But that discounts that Google is looking at that information, right?

MR. JUDISH: Yes.

THE COURT: They're saying Google is the agent. So the government is getting information. They're just only turning it over to another part of the government, the 19 names?

MR. JUDISH: I would not say the government is getting any information about those other people.

THE COURT: I know you wouldn't say that. That wasn't my question. My question was, they're saying that Google is the agent, and so when they're looking at those, that they are at least accessing information about numerous individuals.

MR. JUDISH: Yes, Your Honor. I would note that Google accesses that information anyway. That's how their system works. So Google isn't learning anything it wouldn't use or didn't already know.

It's in their Sensorvault database, which they access frequently for whatever purposes they have. They're looking to try to do what they call semantic information, being able to analyze someone's location history to determine things which would be useful for Google for advertising purposes and stuff like that. So Google looks through the location history. So it's --

THE COURT: So are you saying that Google does that through separate searches, that it's not an algorithm that just works that out? This is different, isn't it? I mean, Google doesn't go in and say, or do they, who is near the federal courthouse so that I can advertise, as a lawyer, on average in a particular period of time?

MR. JUDISH: I think that's exactly what you

can do if you want. That's what Google calls radius targeting. You can say I want --

THE COURT: You can't say "you." You have to say who can say, who's controlling it.

MR. JUDISH: Sorry. An advertiser can say to Google, "I want to target people within a kilometer of the federal courthouse." And then Google will target ads to those people. Google describes this process on its website.

And then afterwards, if you have your law office at some particular place, Google will then do a geofence of people who visit your law office to see those people who it targeted advertisements to, which of them subsequently visit your law office. And then it will tell you how many there are in that. So that really requires Google to do a geofence of people visiting your law office. You know, it's checking to see of these people who they targeted the advertisements to, do they later visit this very specifically defined location. So it's really very closely related to what is done here with a geofence warrant and --

THE COURT: You keep referring to the *Smith* case, and I may not be remembering it well, but didn't the *Smith* case involve use of an operator?

MR. JUDISH: No. No, Your Honor. I mean, it would have been an electronic pen register device in *Smith*.

THE COURT: Okay. All right.

So I'm just going to ask you to address as you go forward, *Carpenter* is focusing on what reveals the privacies of life, right? So I want you to use that lens as you describe to me how you're going through the stages.

MR. JUDISH: All right. So I just want to put on the record one citation before I move on to the three-step process. We talked about where Mr. McGriff explained that location history was the only information sufficiently granular to respond to a geofence warrant. You can find that in his first affidavit, which is Government's Exhibit 3 at paragraph 20.

So the three stages, the three-step process, the first thing I'd say is that I actually, you know, as the Magistrate Judge Harjani in Illinois explained in his opinion, the multi-step process really does lack constitutional significance.

I mean, the key thing here is that we establish probable cause and specify with particularity for all of the information that we

potentially could have obtained. Google very much likes the three-step process. And I think it's an affirmatively good thing that has some additional ability to provide sort of practical privacy protections while still enabling our investigations to proceed. But that doesn't mean that it's constitutionally significant. That's exactly what Magistrate Judge Harjani said. You know, it could have practical benefits, not constitutionally significant. But the key issue before this court is whether the issuing magistrate had a substantial basis for his determination that the evidence the government could potentially obtain was, in fact, evidence of crime and for that reason it established probable cause for it.

But anyway, the way it works is that the first step of the three-step process, all that we got pursuant to that is the latitude and longitude coordinates, which were in the specified geofence, the circle with the radius of 150 meters.

THE COURT: You just, you know, you have to be slower. You just do. Because I don't know what those numbers were. I read them, but our court reporter has to get them as you say them.

MR. JUDISH: All right.

All we get from the first step of the geofence is the latitude and longitude coordinates, which actually fall within the geofence during the hour of the robbery.

So if people, to the extent people came and went from outside during the Step 1 information, we don't get that. It's just if the latitude and longitude points in the Sensorvault database fall within the circle during that hour, then we get those along with an anonymized reference number from which we cannot, without more from Google, determine any identity information.

So that, you know, as far as privacy of life goes, I just don't think that's all that private. Certainly going to a bank is not a particularly private activity.

I do feel obliged to note that I don't think that -- to say *Carpenter* is about protecting the privacies of life, it can't go that far. You'd have to overrule *Smith* and *Miller*. Who you dial on a telephone, that's private. Your financial transactions, those are private things. I think we really do have to take *Carpenter's* word that it's about long-term location information.

But anyway, addressing the Court's question

as to how private the information is, your presence in that 150-meter radius, I think, is not all that private. Obviously, there is a church there. It is hard for me to believe that one can protect oneself from a bank robbery by choosing to rob a bank next to a church and using the church parking lot. And there, I guess, I would point to the Fourth Amendment principle that you can't rely -- it has to be about violation of your Fourth Amendment rights. You don't have standing to challenge Fourth Amendment violations of others.

And whatever the defendant was doing the day of the bank robbery, I don't think he's claimed that he was going to church. So he -- so I don't think that has any impact --

THE COURT: Does he have to claim that? What's his obligation?

MR. JUDISH: I mean, if the issue is to try and assert that his privacy interests were invaded, he needs to explain how his privacy interests were invaded. And so that's the issue which I think he fails on because the defense keeps talking about the potential privacy invasion of people being found inside their home. They don't claim that he was found inside his home. They talk about privacy issues

associated with church. They don't say he was associated with church. He's got to claim his privacy invasion, that his privacy interests were invaded.

So one case I can cite on that is the Seventh Circuit case *Patrick*, which involved use of a cell-site simulator to locate the subject of an arrest warrant. And *Patrick* tried to claim that use of the cell-site simulator violated the privacy interests of others nearby because the cell-site simulator, which is a device which has essentially a direction antenna, which locates where nearby cell phones are, violates the privacy of others nearby.

The Seventh Circuit says no, under *Rakas*, you don't have standing to assert any privacy violations of others.

THE COURT: So are you saying that factually Mr. Chatrie was not in the church?

MR. JUDISH: I don't -- to my knowledge he parked near the church. I have no knowledge that he was in the church. I don't know of anything in the record on that. I mean --

THE COURT: Was he within 2 meters of the church?

MR. JUDISH: He may have been, Your Honor. I don't think -- I think there may be stuff in the

record. I think his coordinates are plotted. And so that would be the place to look for that. I can't state with certainty. So that's the first step.

The second step of the warrant, you know, that enabled the government to get all of the location history over a two-hour interval of the individuals whose information was disclosed in the first step. And so that does, you know, potentially implicate greater privacy interests because you can't have people going to and from the area. But, again, I don't think Mr. Chatrie has pointed out any particularly heightened privacy interests of his which were infringed.

And in any event, I think the real issue is, was there a substantial basis for the magistrate's determination that this would be evidence of crime? And, you know, the additional contextual information is extremely helpful in showing what people's roles in the criminal activity was. And so it was evidence of crime, and therefore appropriately fell within the scope of the warrant.

THE COURT: And so I may be getting ahead of where you are about to argue, but explain to me -- my understanding is that with this degree of certainty of the radius, there is a 150-meter radius, but then a

broader radius that may actually be implicated. Am I right?

MR. JUDISH: Google has, you know, there's chance for errors in the data. There's no question about that. The warrant directed Google to disclose the points where the points calculated by Google fell within the radius, but there was certainly some chance of false positives in that. And, again, I just think that that would go to the weight given the evidence as opposed to whether or not it is actually evidence of crime.

THE COURT: Well, what they're saying is one of the issues is that if you're signing a warrant -- I mean, I think they say it's almost twice as much, like 378 meters, 387 meters, that a magistrate is not on notice that it could be actually twice as large, the area that you're searching, given the rate of potential certainty.

MR. JUDISH: First, I just want to go into the facts. I think they significantly exaggerate the actual inaccuracy. There are a few individual points which have large errors associated with them, but if you look at the actual data, which is in the record, every single one of those will have another point for the same device with the same center and a much

smaller radius.

And as Agent D'Errico testified, what that actually means in practice is that the phone started at the smaller place and then went somewhere, and Google isn't sure where. So it's not that these are devices which may have been the whole time super far away. It's that the way that Google -- you know, they have indication that a device is on the move, but they don't know where. So they, you know, they keep estimating the same center point. But their uncertainty grows.

But the more general point, as far as the magistrate and what was in the affidavit, I think people understand that cell phone measurements are inaccurate, and, thus, I think a commonsense magistrate would know not every location information point is going to be perfect. So I don't think -- and I understand the defense has dropped its argument that it was a, you know, somehow a violation that we didn't include this information in the affidavit. I think that showed up in some of their briefs, but not their final one.

One other point I'd like to make about the three-step process is that it's clear from the Playpen cases that doesn't violate the Fourth Amendment if the

government chooses to obtain less than the maximum amount of information it's authorized to under a warrant.

In the Playpen cases, we were going after a child pornography website on the Dark Web, and we obtained a warrant authorizing us to use code to identify people who logged on to the site. We made explicit in our affidavit that we were authorized to use this code to identify anyone who accessed the site.

We, in fact, were likely to target our code more narrowly than that, and that's ultimately what we did. And this was challenged just as a vast number of cases -- I think there's over 100 Federal District Court cases and there are 11 Federal Court of Appeals cases dealing with challenges to this warrant. I don't think any court has found that that language was problematic.

THE COURT: Well, what is different, though, is that every person who logged on to that account violated the law 100 percent. So not 100 percent of people who were near the bank violated the law, like way, way less than 100 percent.

MR. JUDISH: Yes, that's absolutely right. But the key, what they have in common, is that there

was a substantial basis for the magistrate judge's determination that all of the evidence you're entitled to, all of the information we were entitled to, was evidence of a crime. And that's what counts. And so, again --

THE COURT: It counts because it was an illegal website. How is that not a completely different situation?

MR. JUDISH: Well, the warrants are used to seize evidence of crime, and that can be direct evidence that someone is guilty, but it can also be other information as well. And so the issue is whether a magistrate has a substantial basis to think it was okay or proper that all of the user location information we were authorized to seize would in fact be evidence of crime. It doesn't have to all -- all the people don't have to be guilty. The question is, is what we're authorized to get evidence? And here it was.

It's like I said. It gives us an ability to reconstruct the scene of this crime. It helps us identify accomplices. It helps us find witnesses. It's all appropriate evidence of crime, which can appropriately be seized pursuant to a warrant.

And, yes, there's not all criminals in this

case, but it is all evidence, and as long as we establish probable cause and identify with particularity evidence, I think it's entirely okay for us to then be selective within what the subset of what would establish probable cause and identify with particularity what we ultimately take away.

I think that happens, you know, all the time in search warrants is, you know, we have a warrant. You don't have to, you know, raze a house to find every bit of evidence in a house that you're searching even though, you know, you can keep looking harder and harder and find more of the key thing that you establish probable cause and identify with particularity the things that you are authorized to seize.

In any event, if the Court does have a problem with Step 2 of the warrant, I think the appropriate thing is severance. This is a warrant which is usually conducive to sever. The process was done. The language of the warrant is separate. The process is done in separate steps. This is a warrant which is just enormously easy for the Court to -- would be enormously easy for the standard severance doctrine to apply. From the Step 1 information in this case, it was sufficient to identify which account

likely belongs to the robber, and so the fruit of the poisonous tree would not extend to our subsequent investigation and all of the subsequent evidence we obtained in this case after we first obtained the geofence warrant information.

THE COURT: So you're saying because you had 19 names, you have had enough to identify Mr. Chatrie?

MR. JUDISH: Because we had 19 sets of location information in that 150-meter radius, and we could -- and from the other information obtained at the scene of the robbery, including surveillance videos and eyewitnesses, we knew where Chatrie had come from and, you know, parked, gone into the bank and returned. And the location information of Mr. Chatrie from the geofence warrant was sufficiently consistent with that testimony that we could still tell that he was the one, the robber.

THE COURT: So why did you ask for further information on all 19?

MR. JUDISH: I mean, there's other possibilities which need to be explored, ruled out, like having co-conspirators. And so I think that a lot of that is -- that is helpful to, you know -- investigators tend to be thorough. And they wanted to, you know, be able to get that information because,

you know, some of that information was not entirely inconsistent or, you know, some of that information, you know, suggested that it had some aspect that one might be a co-conspirator like, you know, data suddenly halting suggesting someone turned off their phone.

THE COURT: So, wait. I'm sorry.

MR. JUDISH: I think because there was a possibility of co-conspirators is one possibility to search or to obtain additional information.

THE COURT: So, I guess, then, I'm going to ask you, clearly the terms of the warrant said narrow it down, and your task force officer didn't. And then Google said you have to narrow it down. And explain to me what happened there.

MR. JUDISH: I mean, the warrant says attempt to narrow it down. And, you know, and we ultimately did narrow it down. And so I don't quite -- so, if you look at the actual execution, we did narrow it down. So I don't see any, as an initial matter, I don't see any significance with the, you know, with the fact that it was contemplated to obtain more than we actually did. I don't recall what was in the record regarding why we initially asked for all 19.

THE COURT: Well, I mean, there were other

things in the record like Google saying they didn't think the agent knew what he was doing. That's the only explanation we have it may be wrong, but that is in the record. So --

MR. JUDISH: I don't recall. I mean, I think it's really -- I'm not aware of the Fourth Amendment violation from contemplating but not executing a warrant in an improper way even if it would be improper.

THE COURT: I'm just trying to get the record straight.

MR. JUDISH: I'm sorry. I don't recall.

THE COURT: So how did we get to nine?

MR. JUDISH: Those were the ones which the agent thought were most -- the greatest continued relevance to the case.

THE COURT: And do we know why? Are there parameters that direct to the agent about why?

MR. JUDISH: The warrant very much leaves this to the government's discretion. And I say, again, I think these are of no constitutional significance. You know, part of the reason why is definitely the question of whether these people could actually be additional co-conspirators. And I think that's a primary reason for a continued look at other

suspects.

THE COURT: Okay.

MR. JUDISH: I'll turn now to good faith if you don't have further questions on the warrant itself.

THE COURT: If I do, I'll come back to them.

MR. JUDISH: All right. So, suppression, the Supreme Court has said, is a remedy of last resort and used only where its benefits outweigh its heavy cost. And what you have here really is a new investigative technique.

So when a new investigative technique comes along, there's not a lot of case law to look at because -- well, there's no case law to look at. And so what is an agent supposed to do?

And so the Fourth Circuit looked at this in *McLamb* in the context of the Playpen cases, and what the Fourth Circuit said is that in these, you know, the agent should consult with the expert prosecutors, and if they do that, then it's appropriate to apply in good faith.

Well, it's not because it's not -- they consulted with the prosecutors, and the prosecutors think it's okay. And then they also take it to a judge, and the judge thinks it's okay. And that's

exactly what Agent Hylton did in this case.

And I think it's worth noting, particularly in the context of you going to the state magistrate, that this was not the first time that Hylton had obtained one of these warrants. He had actually gone -- this was his fourth. It actually is in the record, and we've disclosed two of those warrants to the defense. The third remains under seal. That one hasn't been disclosed. But he had previously gone to both a United States magistrate judge and to two Virginia state judges, and they hadn't raised any problems with it. They had signed off on it.

So, what more can an agent do? The prosecutors have no objection to it, a federal judge has no objection to it, two state judges have no objection to it. At this point it's hard to understand why it would be objectively unreasonable for the agent to believe that it's appropriate to seek a geofence warrant.

That is exactly what the Fourth Circuit has suggested that he do. And in *McLamb*, and under those circumstances, suppression, the cost -- the harms of suppression will very much outweigh the benefits. If ultimately the courts -- other courts who look at this decide that it shouldn't be done that way, then,

obviously, it's going to stop.

That's what -- in the *Carpenter* case, that stopped the practice of using historical cell-site location information. But *Carpenter* himself, the Court did not ultimately suppress the cell phone location information obtained and used against *Carpenter* because of the good faith exception.

The benefits don't have to outweigh the harms when you're talking about -- in the context of new investigative techniques. It's also worth noting and closely related to this is we heard from Google more than 8,000 of these over the course of, I believe, a year. So it's clear from that the decisions made by the judges that Hylton has consulted with are not significantly different than the decisions being made by a whole host of other judges around the country, state and federal.

Or, alternatively, we can apply the traditional *Leon* good faith analysis to this. Under the *Leon* good faith analysis, there's no suppression if we rely on good faith on a warrant. And there's a few exceptions to that, but none of those exceptions really apply here.

And one is that the affidavit is so lacking in indicia of probable cause that reliance on the

warrant is unreasonable.

But there is probable cause here. We had a robbery. We had a guy with a cell phone. And the affidavit linked that directly to Google having evidence of the cell phone's location. And that establishes a fair probability that Google had evidence of crime, but it's certainly not wholly lacking in indicia of probable cause. So under the *Leon* good faith, the evidence should not be suppressed.

Similarly, in terms of particularity, the warrant is not so lacking in particularity that reliance is unreasonable. It specifies exactly the information that the warrant is seeking. The two hours of location information or devices which fall within this 150-meter circle during the hour of the robbery. And that's really quite particular. That's stuff that Google's algorithm can go through and separate. It's just -- it's not wholly unreasonable to think that as to a particular warrant, I mean, clearly, some variation of that sort of thing thousands of judges around the country are agreeing that it's appropriate. And at the time there was no contrary decision. And now we have just like a handful of those, like there's three or four

magistrates who have written on this, one of whom thinks it's wholly unreasonable, and others who sort of based on the facts of the case think the government should do a slightly better job. It doesn't suggest that there's anything wholly unreasonable about the government's reliance on the warrant in this case.

So, those cases, you know, generally suggest that, certainly the Weisman decision and the Kansas decision the defense just circulated, suggest that there's nothing fundamentally wrong with geofence warrants. The government just needs to be very careful about establishing probable cause in particularity.

By that standard, the warrant in this case clearly passes the good faith. I mean, the probable cause here is unusually strong because, you know, the robber was seen actually carrying and using a cell phone. That actually hasn't been the cases, in those other cases. They've just tended to make that assumption. But here we've actually got that. So it's just not wholly lacking in probable cause, not wholly lacking in particularity.

And similarly, there's no evidence here that the judge abandoned his judicial role. The judge did what judges are supposed to do. He reviewed the

affidavit and then he signed the warrant. I mean, the kind of case that the Supreme Court talks about for someone abandoning their judicial role is the case -- the example they give is *Leon*. And what that actually involves is a judge who decided to help with the execution of the warrant, that he actually went to the scene to be searched and decided what could and couldn't be seized.

Well, that's what the Supreme Court means when it says a judge who abandons his judicial role, you know, that you don't apply the *Leon* good faith. And there's nothing like that here. This magistrate reviewed the warrant affidavit and signed the warrant, and that's entirely appropriate, and so *Leon* good faith applies in this case.

And if you don't have any further questions, we'd ask the Court to deny the suppression motion.

THE COURT: I do have a question. I think I can discern from what you're arguing what case you think I should rely on for purposes of my evaluation of this case, but why don't you just tell me on the record.

MR. JUDISH: The Harjani opinion is one geofence case issued by a magistrate judge who bothered to write up his opinion, and I think that

there's a lot to commend that. And there's also the cell-tower dump. *James* is reasonable similar as a case, you know, at least involving evaluation of probable cause and particularity.

The District Court opinion in that case finds that cell-tower dump warrants are appropriate.

THE COURT: All right. So I think I've heard maybe both sides a little bit talk around or near or maybe directly suggest two things. One is that this warrant might be stronger if Google stored its information in a different way, if it was stored by location. So the question is, what's the upshot of that? Does any court have the power to say that? Would there have to be a congressional determination to make that happen? And I think I want to ask generally, I see that the government is steering away from the Stored Communications Act, and I want to confirm that you are resting this entirely on a constitutional analysis.

I mean, one of the issues is, of course, right, there is no statute that addresses geofencing. Right? And, in fact, there's been no statute addressing almost any more recent electronic surveillance process because it develops so quickly that almost as soon as something gets passed, say, in

two and a half years, it's obsolete.

So I want to hear what you have to say about what I have the power to do or the appropriate action I should be taking, and if there's any statutory obligation with respect to what's going on.

MR. JUDISH: I do think they'll start with the Stored Communications Act part. I do think this compelled disclosure of the information is governed by the Stored Communications Act. I just don't think it matters for purposes of a motion to suppress because the act itself has no statutory suppression remedy. And so it just doesn't matter.

Whenever you get into a Fourth Amendment -- the Stored Communications Act matters enormously --

THE COURT: Wait. You have to slow down.

MR. JUDISH: Sorry.

THE COURT: Okay. Just start right over and act like I don't know what you're about to say.

MR. JUDISH: All right.

The Stored Communications Act contains no suppression remedy. It contains a section 18 U.S.C. Section 2707, which specifies that the remedies in the statute are the only available remedies for the violation of the statute. And 2707 includes various damages provisions, but not a suppression remedy. And

there are various cases confirming, in fact, there is no suppression for a statutory violation.

And, you know, I think the *Smith* case in the Ninth Circuit, I think. Anyway, but here because the only issue for this court is whether the evidence should be suppressed, the Court just doesn't need to focus deeply on the questions of how this information falls within the --

THE COURT: Does it need to or can't?

MR. JUDISH: I'm not sure why it would be relevant. I mean, you certainly -- I'm never going to tell a judge what it can or can't do. But I just don't see the relevance to this case. I mean, sometimes we can argue that that's an additional reason against suppression. But, you know, like a good faith reliance on a statute. But here the government has not advanced that position. We have argued good faith based on *Leon*.

So -- and as far as the structure of Google's database, I don't think, you know, I never want to willingly waive the government's authorities or powers, but I'm certainly not in a position of making any claim that a court has authority to tell them how to structure their database.

I think the main argument that we make based

on the structure of their database is the argument that Fourth Amendment rights should not turn on internal prior practices which are not visible to the public, and the structure of their database is one of those things. And, thus, the fact that this could be done in a way which would allow Google to -- Google's machines to filter very narrowly, strongly suggests that there is no search of millions of people when its database requires a broader filter.

THE COURT: And with respect to -- does the government have any position about whether or not a review at each step by a neutral magistrate would be necessary or beneficial or better?

MR. JUDISH: I mean, I think if we can, as I believe we did here, establish probable cause for all of the evidence from the start, it's fine to do so. I don't think it does any harm to have additional steps. It could be structured to require to have a magistrate make an additional finding along the way, and there would be no problem with that.

So I think it's not necessary, but not in any way problematic to involve a magistrate in multiple decisions.

THE COURT: Right. And so if -- I guess I want you to unpack exactly why the ability to delete

the information, if Mr. Chatrie could figure that out, how it affects my analysis.

MR. JUDISH: I think one way it affects your analysis is it distinguishes this from *Carpenter* and why *Carpenter* said the third-party doctrine didn't apply. *Carpenter* had three reasons for why third party didn't apply to cell-site information. One of them was that it could be deleted.

THE COURT: All right. And so I'm not quite sure how to phrase this, but -- so if there's probable cause here, obviously, there's video surveillance that a robbery occurred. Is the government's position that there would still be probable cause to do this geofence if there were no video or any indication that Mr. Chatrie had a phone?

MR. JUDISH: It can be. I mean, cell-tower dumps in the *James* case, for example, there was no evidence that the defendant had a phone, and the Court still found that probable cause was established. I mean, probable cause is a common sense determination by the magistrate whether there's a fair probability that the target had prior evidence of crime. And so you certainly can have that.

In another of the cases, I think the Harjani opinion, that involves criminal activity of the sort

that it looks like it was probably more than one person involved, and so that gives rise to an inference of a likely cooperation among people, and people use cell phones to communicate and cooperate. So you have to look at the facts of any particular case and make a determination of whether they establish a fair probability.

So sometimes I think you can establish probable cause regardless of whether a person has a phone. It's really --

THE COURT: So I guess I'm trying to find out where it stops. Like when don't you have probable cause if you don't have evidence of using a phone, probable cause for a geofence?

MR. JUDISH: I think it's really -- it's -- I think it just depends on the facts of the case and whether you think there will be evidence of crime. And this is a determination made by magistrate judges. This court obviously doesn't need to confront that in this case because this is a case with a cell phone. But I do think that, you know, the fact that if there really is, you know, a fair probability that Google will have location information of someone who committed a crime, a warrant should issue, and it shouldn't be an argument that, well, that happens a

lot. It is true that we're able to solve lots of crimes because we establish probable cause in lots of circumstances. That is an affirmatively good thing.

So I don't think that an argument I've seen from at least one magistrate judge in the recent Kansas opinion that we can't have too many of these geofence warrants is correct. I think the issue is, can we establish probable cause? And you can't say this isn't probable cause because you're going to solve too many crimes that way.

THE COURT: I think that's a little different from saying when isn't there probable cause, right? I mean, no one is going to say let's not solve crimes. Right?

MR. JUDISH: Right.

THE COURT: Defense counsel is not going to say that. That's not what they're arguing.

MR. JUDISH: I apologize, Your Honor. I guess the way I should say it, the Court seems to think that warrants shouldn't issue because they would issue in too many cases, and -- but that's not --

THE COURT: I'm not asking that question. I'm asking when doesn't it issue? I'm saying, give me an example.

MR. JUDISH: I mean, there's -- I mean, I

guess you could have an example where it's clear that a guy wasn't carrying a cell phone. You know, if someone walks in with, you know, pocketless gym shorts and a T-shirt and commits a crime, you can probably tell by looking at him or from video surveillance footage that there is no phone on this guy. And in that case, I think there wouldn't be probable cause.

THE COURT: All right. Okay. I think that's it.

MR. JUDISH: All right. Thank you, Your Honor.

THE COURT: Can I ask you how long you think your response is going to be?

MR. PRICE: I will try and keep it very brief, Your Honor.

THE COURT: Well, that is about as particular as whether it's granular.

MR. PRICE: Sorry about that. I have three points. I think less than 10 minutes.

THE COURT: Okay.

MR. PRICE: Counsel tells me maybe 15.

THE COURT: Maybe 15. All right. I'm going to give Ms. Daffron a little bit of a break. I just think that, you know, maybe she'll buy me a cupcake after.

All right. We'll take a 15-minute recess.

(Recess taken from 2:22 p.m. until **2:40 p.m.**)

MR. JUDISH: Your Honor, I just want to make -- correct the transcript in one place. I did not do a great job explaining this.

THE COURT: That's fine. Please approach the podium to do that.

MR. JUDISH: Thank you, Your Honor.

Regarding the reasons behind the second stage of the search, they are explained by Agent D'Errico at page 546 of the transcript. So I'll stop there.

THE COURT: Wait. I'm sorry.

MR. JUDISH: Okay. So -- all right. I won't stop there.

THE COURT: Yes.

MR. JUDISH: So, Agent D'Errico was asked why go back at the second stage. And at 546, he says there are several reasons. I know I need to talk more slowly. I'm sorry.

So the first reason is, this is a device that was present in the area of the bank prior to the bank robbery. And we know that sometimes when people want to hide their location, they will turn their phones off. And if their phone is turned off, no additional location history would be reported for that device.

So it's significant to us that there is a point inside the geofence that occurred prior to the bank robbery with no points after the bank robbery because we also believe that after a subject has robbed a bank, that they are going to flee the area and not have any additional location history records within the geofence several minutes after the bank robbery.

THE COURT: All right.

MR. JUDISH: That's all, Your Honor.

THE COURT: All right. Thank you, sir.

MR. PRICE: Good afternoon, Your Honor. Can you hear me okay?

THE COURT: I can.

MR. PRICE: All right. I'd like to begin by correcting a few points for the record.

The first is that radius targeting, which is that form of advertising the government was talking about, does not use location history according to Google.

THE COURT: Wait. Say that again. Radius --

MR. PRICE: Radius targeting, this idea that you can advertise to everybody around the courthouse if you're a lawyer. While that may be possible, Google has stated -- it's at page 197 to 98 of the transcript -- that location history is not used for

that purpose.

Second, with respect to traffic predictions, once again, pages 407 to 408 of the transcript explains how Google does not use location history but uses aggregated data and percentages with added, quote, noise to prevent any possibility of ID'ing individual devices.

And then, finally, with respect to the questions about how the government narrowed things down in Step 2 and then Step 3, we should note that one of the three finalists, so to speak, was, in fact, one of the false positives. So somebody who was just driving by, likely never within that geofence at all, and was reported as being inside of it, therefore it had Stage 2 data under the government's reveal, and then Stage 3 data as well. That was one of the false positives.

THE COURT: Okay.

MR. PRICE: So I want to touch briefly on a few points.

First, this idea that location history is voluntary because of the process involved, and the mere fact that it is stored with Google, a third party.

Almost everything the government said about

the voluntariness of enabling location history can be said of Gmail, of Google email. It is stored by Google. It is transmitted by Google. Google advertises off of emails. And yet even the government agrees that email deserves Fourth Amendment protection. I suppose they have to after the Six Circuit's decision in *Warshak* and their representation to the Supreme Court in *Carpenter* that email requires a warrant to get.

That is not something that the Supreme Court has weighed in on. And under a strict reading of the Stored Communications Act, as it still exists, the government did, in fact, argue they did not need a warrant to obtain email that was older than 180 days.

The Sixth Circuit in *United States v. Warshak* found that email, despite being housed on Google's servers or on other servers, deserved the same kind of privacy as one's papers and effects. That is the modern day scion of one's private papers and effects.

All of those points we can attribute, as well, to location history. The Stored Communications Act, while not determinative, is certainly relevant to the reasonable expectation of privacy analysis.

Google considers location history to be content and users understand that content is their

data and it is protected from unauthorized disclosure.

Likewise, this is different from a subpoena, fundamentally different from a subpoena, because Google is not searching its own business records. The government is not asking to search preexisting records that Google already has in the same way that a cell company might have data about how many people use a tower in order to figure out whether to add another tower or why calls might be getting dropped.

Google never runs a search to figure out who was around the bank or who was around. They don't have towers. They have no need for this, to have location data sorted by location. It is considered, once again, user content, and that is why the database -- the Sensorvault is structured in that way. It is a reflection of this idea that location history is content. It belongs to users. It is their data. They can manipulate it. They can delete it. It is not Google's data.

I want to touch briefly on the idea that *Carpenter* hasn't been applied or expanded since *Carpenter* was decided. The government cites *Hammond*, which is a case about realtime cell-site information, as well as historical cell-site information; 127 days of it actually. And there the Court found that a

search of the 127 days of historical cell-site information was a search, but that the good faith doctrine applied. Why? Because the 2703(d) order was issued prior to *Carpenter* being decided.

So, in fact, the vast majority of cases that have been decided since *Carpenter* follow a similar pattern recognizing that these cases take some time to percolate up. And some of the searches that we're still seeing right now were executed prior to June of 2018.

So those cases are just coming up now, and the vast majority of them holding that *Carpenter* doesn't apply do so on good faith grounds.

The other case that the government cites, also a Seventh Circuit case, *Adkinson*, did involve a tower dump, but the government didn't conduct it. The suspect in that case, the defendant in that case, was accused of robbing multiple T-Mobile stores. So T-Mobile, on its own, looked at its own cell-site records to try and figure out which T-Mobile customers had used their towers near those stores. So it wasn't government action in the same way that we have here.

And I think that leads in nicely to this larger point that Google was acting as a government agent. There would be no Step 1 data without Google's

participation. And Google would not have done any of this had it not received compulsory legal process. Google, in this sense, can't be anything but a government agent at Step 1. The government is outsourcing the search function to Google. It's that simple.

Finally, I want to touch on the *McLamb* Playpen good faith argument. As Your Honor correctly pointed out, that case turned -- was based on the fact that there was probable cause for every computer that was searched. So the issue there was not probable cause. The issue in *McLamb* was a very complicated jurisdictional question about the reach of Rule 41 and whether judges in one district could issue warrants that applied extraterritorially to other jurisdictions.

At the time there were multiple conflicting court decisions in the country about this. And it was, admittedly, something of a close call. So in that case, consulting with attorneys and prosecutors would make a lot of sense. But there was no question about whether probable cause was necessary. That is a fundamental question, a fundamental Fourth Amendment question that has to be answered in every single case. And it is antithetical, I think, to the Fourth

Amendment to say that the government can get away with a warrant that doesn't have probable cause or lacks particularity simply because they checked with the prosecutor.

That rule, if read that broadly, would eviscerate the Fourth Amendment. Anything that a government agent wanted to do, they could just clear with the prosecutor, and so it would be good faith at the end of the day. I don't think that's the rule in *McLamb*.

Once again, the Court was not looking at a basic question like were these warrants supported by probable cause. It was a very technical, legal question about the reach of Rule 41.

THE COURT: Well, to be clear, they're saying that, regardless of anything in *McLamb*, they had probable cause here because they had a video of somebody robbing a bank using a phone.

MR. PRICE: I don't think that having a phone in and of itself is enough to establish probable cause. If only a third of Google users have location history enabled, and not all people who have cell phones have Google phones, and some of the people who, because of the way that the 68, 32 percent error rate works, at least some of those people who might have

been there will not show up there within the geofence because of this idea of false positives and false negatives. So I think there's actually a few more steps to do to go from having a phone to probable cause.

And as we know from *Riley*, and the government's own statistics, having a cell phone is a fairly common thing. And I have no doubt that in a case where the suspect was not seen with a cell phone, perhaps wearing gym shorts and a T-shirt, that the government would say he left the phone in his car or that they might need to get a warrant or look for witnesses or co-conspirators anyways.

I think there is a lot of work to be done on the probable cause front to go from a cell phone was seen to there's probable cause for searching location history.

THE COURT: Okay.

MR. PRICE: That's all. Thank you very much, Your Honor.

THE COURT: I'm going to ask you one question based on their argument. It seems that part of what they're saying is that the probable cause was based on the fact that there was a crime and that getting the results of the geofence would help reconstruct the

crime. That it's just an investigative tool. And so there's probable cause to know that the way that folks were operating around, it's just a different type of surveillance, and that it would, at least probably, show evidence that a crime had been committed.

MR. PRICE: I think there's a lot of information that might be helpful in the abstract. And nobody is preventing the government from obtaining this information. The idea is simply that they must have probable cause to do it.

So it may be useful to get the location history data of people inside the bank, but then identify those people inside the bank and seek a warrant for their location history information if all you're trying to do is just get a better sense of the scene. In the same way that you would go and identify the surveillance cameras in the area and get the video from there, you wouldn't start with every surveillance video camera in the country, and then narrow it down to the ones around the bank.

So I think while there may be lots of information that's useful in terms of solving crimes, the Fourth Amendment limits what the government can get based on probable cause and particularity. Thank you.

THE COURT: Thank you.

All right. Well, I want to thank you all for your efforts and for your argument.

I am, not surprisingly, going to issue a written opinion. You all have submitted lots of documents, and I've heard testimony, and I want to be sure you have a decision that you can read and either agree with or disagree with, and then move on from there.

I certainly will do so as swiftly as I can. And, certainly, we've been working on it, and we will continue working on it. So we're not behind the ball, but we're not where you guys are. We haven't finishing our briefing.

So how is it, with that understood, how is it that you want to proceed?

MS. KOENIG: Good afternoon, Your Honor.

THE COURT: Good afternoon.

MS. KOENIG: I think Ms. Daffron is probably grateful that I wasn't talking very much today.

But I think in terms of the defense perspective, obviously there are other motions that are pending. I will say that the Court's determination of this motion, I think, will make dispositive some other issues in the case regardless

of how the Court rules.

So from the defense perspective, I would ask that the Court continue to hold the other motions in abeyance until after the decision on this motion. I don't believe at this point we need to reset a trial, but if that becomes necessary, obviously we can do that once the Court makes a decision.

THE COURT: Right. Does the government have a perspective?

MR. SIMON: Judge, we don't mind the Court holding those motions in abeyance. To the extent the Court wanted to rule from the four corners of the search warrant, I don't believe we intend to elicit additional evidence on those motions. So we'll just defer to the Court on whether it holds it in abeyance or not.

THE COURT: All right.

Well, what I will certainly do is not rule on those issues without notice. I think that's fair. And so I will decide this particular motion, which is clearly the heart of what we're discussing, and then we will handle the other motions accordingly, but not by surprise. So you can presume that I would handle it that way.

I'm not going to schedule a trial date. So

this means that this motion is under advisement, including all the findings that I've made with respect to the complexity of the case, the fact that we've had testimony from across the country, unusual sets of affidavits.

It is the fact that the speedy trial continues to be held in abeyance for a bit because it outweighs the public's interest in a speedy trial, and Mr. Chatrie's, given the weight and the seriousness of the issues before me.

But I do tell you all that we are on it, and I am aware that, especially with COVID and with folks being unable to travel from California to testify in person, that this is an unusually long pendency in a case, and I am taking that into account as I approach it. All right?

Is there anything else I need to cover?

MR. SIMON: Nothing further, Judge.

MS. KOENIG: Not from the defense, Your Honor. Thank you.

THE COURT: All right. Well, you all have done a tremendous job. And thank you for your time, and I will issue my opinion. Thank you.

(The proceedings were adjourned at 3:00 p.m.)

I, Diane J. Daffron, certify that the foregoing is

a correct transcript from the record of proceedings in the above-entitled matter.

/s/

_____ _____

DIANE J. DAFFRON, RPR, CCR DATE

This page intentionally left blank for double-sided pagination and printing

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Richmond Division (The Hon. M. Hannah Lauck)

JOINT APPENDIX

VOLUME 6 of 11 (pages 1327 - 1456)

JESSICA D. ABER
United States Attorney

Kenneth R. Simon, Jr., Ass't U.S. Attorney
Peter S. Duffey, Ass't U.S. Attorney
Counsel for Appellee
919 East Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400

Nathan P. Judish, Senior Counsel
Computer Crime & Intel. Property Section
Criminal Division
U.S. Department of Justice

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
Counsel for Appellant
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800

Michael W. Price, Litigation Dir.
NACDL Fourth Amendment Ctr.
1660 L Street NW, 12th Floor
Washington, DC 20036

This page intentionally left blank for double-sided pagination and printing

TABLE OF CONTENTS

VOLUME 1 (pages 1 - 176)

District Court Docket Sheet (as of Jan. 17, 2023) 1

Indictment (Sept. 17, 2019, Doc. 1).....22

Defendant's Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Oct. 29, 2019, Doc. 29) 25

Government's Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (Nov. 19, 2019, Doc. 41) 51

Defendant's Reply to Government's Response [to] Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Dec. 9, 2019, Doc. 48).....76

Exh. A (First Step 2 Request to Google) (Doc. 48-1) 98
Exh. B (Second Step 2 Request to Google) (Doc. 48-2) 100
Exh. C (Third Step 2 Request to Google) (Doc. 48-3) 102
Exh. D (Transcript, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019)) (Doc. 48-4)..... omitted from J.A.

Government's Notice Regarding Attachment of Google Geofence State Search Warrant to Response in Opposition to Motion to Suppress (Dec. 18, 2019, Doc. 54) 104

Affidavit for search warrant and warrant, with attachments (Doc. 54-1) 107

Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant (Dec. 20, 2019, Doc. 59-1) 118

United States' Response to Amicus Curiae Brief of Google LLC (Jan. 10, 2020, Doc. 71).....148

Defendant's Response to Google's Motion to File Amicus Curiae Brief in Support of Neither Party (Jan. 10, 2020, Doc. 72) 158

VOLUME 2 (pages 177 - 416)

Transcript, Discovery Motion Hearing (Jan. 21, 2020, Doc. 81; *see* Doc. 77 (court minutes))....177

Preliminary matters....179

Def't witness Spencer McInvaille — Direct examination....193; Cross examination....283; Redirect examination....306

Argument by the defense....318
Argument by the government....332
Rebuttal by the defense....350

Court's ruling....355

Defendant's Supplemental Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (May 22, 2020, Doc. 104)....363

United States' Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (June 12, 2020, Doc. 109)....393

VOLUME 3 (pages 417 - 694)

Transcript, Suppression Motion Hearing, Day 1 (evidence) (Mar. 4, 2021, Doc. 201; *see* Doc. 198 (court minutes))....417

Preliminary matters....420

Def't witness Spencer McInvaille — Direct examination....432; Cross examination....542; Redirect examination....586

Def't witness Marlo McGriff — Direct examination....606

VOLUME 4 (pages 695 - 1070)

Transcript, Suppression Motion Hearing, Day 2 (evidence) (Mar. 5, 2021, Doc. 202; *see* Doc. 199 (court minutes)) 695

Preliminary matters 698

Def't witness Marlo McGriff, cont'd — Direct examination ..... 699; Cross examination ..... 791; Redirect examination 841

Def't witness Sarah Rodriguez — Direct examination ..... 862; Cross examination ..... 902; Redirect examination 916

Gov't witness Jeremy D'Errico — Direct examination ..... 923; Cross examination ..... 967; Redirect examination 1010

Gov't witness Joshua Hylton — Direct examination ..... 1016; Cross examination ..... 1040; Redirect examination 1063

Concluding matters 1064

VOLUME 5 (pages 1071 - 1326)

Defendant's Post-Hearing Brief on "Geofence" General Warrant (May 3, 2021, Doc. 205) 1071

Government's Response in Opposition to Defendant's Motion for Suppression (May 21, 2020, Doc. 214; *see* Doc. 207-2) 1117

Defendant's Reply to Government's Response in Opposition to Motion for Suppression (June 4, 2020, Doc. 213) 1164

Transcript, Suppression Hearing (arguments) (June 24, 2021, Doc. 217; *see* Doc. 215 (court minutes)) 1185

Argument by the defense 1187
Argument by the government 1231
Rebuttal by the defense 1313

Concluding matters 1322

VOLUME 6 (pages 1327 - 1456)

Memorandum Opinion (denying suppression motion) (Mar. 3, 2022, Doc. 220) 1327

Order (denying suppression motion) (Mar. 3, 2022, Doc. 221) 1390

Criminal Information (May 6, 2022, Doc. 224) 1391

Transcript, Change of Plea Hearing (May 9, 2022, Doc. 247; *see* Doc. 226) 1394

Plea Agreement (May 9, 2022, Doc. 228) 1428

Statement of Facts (May 9, 2022, Doc. 229) 1444

Judgment in a Criminal Case (Aug. 19, 2022, Doc. 239) 1449

Notice of Appeal (Aug. 25, 2022, Doc. 241) 1456

VOLUME 7 (pages 1457 - 1810) – DOCUMENT EXHIBITS

Exhibits Admitted at Discovery Motion Hearing (Jan. 21, 2020)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) ..... *see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) ..... *see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) ..... *see* J.A. 2093
Def't Exh. 4: Activation Video ..... omitted from J.A., available on request
Def't Exh. 5: Three Paths Video (sealed) ..... *see* J.A. 2139
Def't Exh. 6: First Step 2 Request to Google 1457
Def't Exh. 7: Second Step 2 Request to Google 1459
Def't Exh. 8: Third Step 2 Request to Google 1461

Def't Exh. 9: Step 3 Request to Google 1463

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) .....*see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) .....*see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) .....*see* J.A. 2093
Def't Exh. 5: Three Paths Video (sealed) .....*see* J.A. 2139
Def't Exh. 6: Spencer McInvaille Report 1464
Def't Exh. 7: Spencer McInvaille Supplemental Report 1469
Def't Exh. 8: CSV Google Data File (.csv file) .....*see* J.A. 2139
Def't Exh. 9: Unique in Crowd Study 1475
Def't Exh. 11: September 2018 Oracle Submission 1480
Def't Exh. 18: Federal Search Warrant Application & Attachments 1502
Def't Exh. 19: State Search Warrants & Attachments 1534
Def't Exh. 21: McGriff Declaration 1 (Doc. 96-1) 1551
Def't Exh. 23: McGriff Declaration 3 (Doc. 147) 1562
Def't Exh. 24: Rodriguez Declaration (Doc. 96-2) 1579
Def't Exh. 27: Every Step You Take 1587
Def't Exh. 30: AZ Ex. 18 (admitted portions only) 1631
Def't Exh. 31: AZ Ex. 19 (admitted portions only) 1633
Def't Exh. 32: AZ Ex. 20 1639
Def't Exh. 33: AZ Ex. 24 1644
Def't Exh. 34: AZ Ex. 202 1667
Def't Exh. 36: AZ Ex. 209 1777
Def't Exh. 38: AZ Ex. 219 1781
Def't Exh. 40: AZ Ex. 236 1797
Def't Exh. 41: AZ Ex. 260 1804

VOLUME 8 (pages 1811 - 2090) – DOCUMENT EXHIBITS, CONT'D

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021), cont'd

Def't Exh. 43: May 2018 Privacy Policy – Redline 1811
Def't Exh. 43a: May 2018 Privacy Policy – Redline (with internet source information) 1840
Def't Exh. 44: Jan. 2019 Privacy Policy – Redline 1865
Def't Exh. 45: Oct. 2019 Privacy Policy – Redline 1895
Def't Exh. 46: McGriff Blog 1 1926

Def't Exh. 47: McGriff Blog 2 1929
Def't Exh. 48: 2018 Quartz Article 1934
Def't Exh. 49: 2018 AP Article 1 1941
Def't Exh. 51: 2019 NYT Article 1948
Def't Exh. 53: Blumenthal-Markey Letter to FTC 1957

Gov't Exh. 1: CAST PowerPoint Presentation 1981
Gov't Exh. 2: Geofence Warrant (Doc. 54-1) ..... *see* J.A. 107
Gov't Exh. 3: Declaration of Marlo McGriff (Mar. 11, 2020)
(same as Def't Exh. 21 (Doc. 96-1)) ..... *see* J.A. 1551
Gov't Exh. 3a: Declaration of Sarah Rodriguez (Mar. 11, 2020)
(same as Def't Exh. 24 (Doc. 96-2)) ..... *see* J.A. 1579
Gov't Exh. 3b: Supplemental Declaration of McGriff (June 17, 2020)
(Doc. 110-1) 2032
Gov't Exh. 3c: Third Declaration of Marlo McGriff (Aug. 7, 2020)
(same as Def't Exh. 23 (Doc. 147)) ..... *see* J.A. 1562
Gov't Exh. 4: Joshua Hylton emails with Google 2034
Gov't Exh. 5: Google Privacy Policy 2048
Gov't Exh. 5a: Google Terms of Service 2081
Gov't Exh. 6: Special Agent D'Errico's C.V. 2088
Gov't Exh. 12: "Got to Be Mobile" Video ..... *see* J.A. 2091

VOLUME 9 (pages 2091 - 2092) – DIGITAL MEDIA EXHIBIT

Gov't Exh. 12: "Got to Be Mobile" Video (admitted only at suppression motion hearing) ..... (.mp4 file)

VOLUME 10 (pages 2093 - 2138) – SEALED DOCUMENT EXHIBIT

Def't Exh. 3: PDF of Raw Data (*see* Doc. 69 (sealing order)) (admitted at both discovery motion hearing and suppression motion hearing) 2093

VOLUME 11 (pages 2139 - end) – SEALED DIGITAL MEDIA EXHIBITS

Def't Exh. 5: Three Paths Video (admitted at both discovery motion hearing and suppression motion hearing) ..... (.mp4 file)
Def't Exh. 8: CSV Google Data File (admitted only at suppression motion hearing) ..... (.csv file, viewable in Excel)

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA

v. **Criminal Case No. 3:19cr130**

OKELLO T. CHATRIE,

Defendant.

MEMORANDUM OPINION

I. Introduction

Ratified in 1791, the Fourth Amendment to the United States Constitution guarantees to the people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. To that end, the Framers prohibited the issuance of a warrant, unless that warrant was based "upon probable cause" and unless it "particularly describ[ed] the place to be searched, and the persons or things to be seized." *Id.* The Supreme Court of the United States has since applied the principles embodied in this language to constantly evolving technology—from recording devices in public telephone booths, *Katz v. United States*, 389 U.S. 347 (1967); to thermal-imaging equipment, *Kyllo v. United States*, 533 U.S. 27 (2001); and, most recently, to cell-site location data, *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

This case implicates the next phase in the courts' ongoing efforts to apply the tenets underlying the Fourth Amendment to previously unimaginable investigatory methods. In recent years, technology giant Google (and others) have begun collecting detailed swaths of location data from their users. Law enforcement has seized upon the opportunity presented by this informational stockpile, crafting "geofence" warrants that seek location data for every user

within a particular area over a particular span of time. In the coming years, further case law will refine precisely whether and to what extent geofence warrants are permissible under the Fourth Amendment. In the instant case, although the Motion to Suppress must ultimately be denied, the Court concludes that this particular geofence warrant plainly violates the rights enshrined in that Amendment.

II. Findings of Fact and Procedural History

A. Findings of Fact[1]

1. The Robbery at the Call Federal Credit Union

On May 20, 2019, at approximately 4:52 p.m., a bank robbery occurred at the Call Federal Credit Union (the "Bank") in Midlothian, Virginia. The suspect held a firearm over the course of the robbery and took $195,000 from the Bank.

During the robbery, the suspect presented a teller working at the Bank a handwritten note that stated:

> I've been watching you for sometime [sic] now. I got your family as hostage and I know where you live, [i]f you or your coworker alert the cops or anyone your family and you are going to be hurt. I got my boys on the lookout out side [sic]. The first cop car they see am going to start hurting everyone in sight, hand over all the cash, I need at least 100k and nobody will get hurt and your family will be set free. Think smartly everyone['s] safety is depending and you and your coworker[']s action so I hope they don't try nothing stupid.

[1] A "presumption of validity" exists "with respect to the affidavit supporting the search warrant." *Franks v. Delaware*, 438 U.S. 154, 171 (1978). Because Chatrie does not allege that the statements in the affidavits supporting the search warrants are untrue statements, but instead says that these statements do not provide enough information or that they do not contain the proper information to support the search warrants, the Court in part makes its findings of fact based on the statements made in the affidavits. *Id.* (describing the circumstances in which the Court must hold an evidentiary hearing on a defendant's motion to suppress).

(ECF No. 54-1, at 6.)[2] The teller told the suspect that she did not have access to that amount of money, and the suspect then displayed a silver and black firearm. While openly holding the gun, the suspect directed the teller, other Bank employees, and the Bank customers to move to the center of the lobby and get on the floor. The suspect then led these individuals behind the teller counter to an area that contained the Bank's safe. Once behind the counter, the suspect forced the Bank's manager to open the safe and place $195,000 into a bag he brought with him. After acquiring the money, the suspect left the Bank on foot, "towards an adjacent business, west of the [B]ank." (ECF No. 54-1, at 6.)

During its investigation, law enforcement obtained the instant Geofence Warrant (hereinafter "Geofence Warrant" or "Warrant")—a novel application of search technology whose use has grown exponentially in recent years. Google produced certain location information pursuant to the Warrant, which led the police to Okello Chatrie. Chatrie was eventually charged with two crimes related to the robbery.[3] He then filed a Motion to Suppress the Geofence Warrant that forms the basis of this Opinion.

---

[2] The Court employs the pagination assigned by the CM/ECF docketing system for citations to the parties' submissions. Where a document was not filed through CM/ECF (for example, an exhibit introduced at a hearing), the Court will cite to the pages that would have been assigned through CM/ECF had they been filed through the system.

In addition, the Court acknowledges that its findings of fact differ between this Memorandum Opinion and a later issued Memorandum Opinion addressing the validity of four other warrants. In that Opinion, the warrants set forth a lengthier, more detailed narrative explaining the officers' investigatory steps than the instant Geofence Warrant. In determining the validity of a warrant, the "magistrate [or magistrate judge], and a reviewing court, will restrict their inquiries on probable cause to the facts set forth in the four corners of the officers' sworn affidavit." *United States v. Lipscomb*, 368 F. Supp. 3d 680, 684 (E.D. Va. 2019). Thus, because the facts in the Geofence Warrant differ from those set out in the four other warrants, the Court's findings of fact accordingly differ as well.

[3] More precisely, (1) Forced Accompaniment During Armed Credit Union Robbery, in violation of 18 U.S.C. §§ 2113(a), (d), and (e); and, (2) Using, Carrying, or Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A).

2. The Record Presented to the Court by the Parties

There is a relative dearth of case law addressing geofence warrants.[4] In this case, the parties, especially the defense, pursued a thorough and deep record. This Court was aided by Amicus Google's provision of detailed information, including in-person testimony regarding the company's acquisition, retention, and use of users' location data. In what may be a first, Google filed an Amicus Brief.[5] Mr. Marlo McGriff, a Location History Manager at Google since 2016, submitted three declarations over the course of this matter. Ms. Sarah Rodriguez, a Team Lead for Legal Investigations Specialists ("LIS")[6] at Google since 2018, provided one declaration. During a hearing on March 4–5, 2021, (one of many in this case), the Court heard live testimony from both Mr. McGriff and Ms. Rodriguez.[7]

---

[4] Specifically, this Court has identified only five other federal opinions on the subject, but all assessed the validity of the warrants *before* they were issued: *In re Search of Information That is Stored at the Premises Controlled by Google LLC*, No. 21sc3217, 2021 WL 6196136 (D.D.C. Dec. 30, 2021); *In re Search of Information that is Stored at the Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153 (D. Kan. 2021); *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); and, *In re Search of Information Stored at Premises Controlled by Google*, No. 20M297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).

[5] Among other things, Google argued in its brief that Location History is not a business record, but is a journal stored primarily for the user's benefit and is controlled by the user. Google states that LH information "can often reveal a user's location and movements with a much higher degree of precision than [Cell Site Location Information]." (ECF No. 59-1, at 8.) Google argues that a geofence is certainly a "'search' within the meaning of the Fourth Amendment," because "[u]sers have a reasonable expectation of privacy in the LH information, which the government can use to retrospectively reconstruct a person's movements in granular detail." (ECF No. 59-1, at 9.)

[6] Legal Investigations Specialists are the Google employees who receive warrants and send the returns.

[7] This testimony was delayed at the request of defense counsel during an extensive period of time because the COVID pandemic prevented live testimony.

The parties to this case also brought their own experts. Spencer McInvaille, an expert in digital forensic examinations, forensics, and cellular location testified for the defense, and FBI Special Agent Jeremy D'Errico, a part of the cellular analysis survey team ("CAST") spoke for the Government. Multiple rounds of briefing occurred before, during, and after the hearings held by the Court.

In order to establish as thorough a record as possible with respect to this new technology, the Court will first discuss Google's location services, as well as Google's typical response to geofence warrants.[8]

3. Google's Collection and Production of Location Data

a. Google's Suite of Location Services

Google collects detailed location data on "numerous tens of millions" of its users. (ECF No. 96-1, at ¶ 13; ECF No. 201, at 205.) It acquires and stores this data through one of at least three services: (1) Location History, (2) Web and App Activity ("WAA"), and (3) Google Location Accuracy ("GLA"). Google only searches Location History when it receives a geofence warrant.

i. Location History

Location History appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing *location* data. Google developed Location History to allow users to view their Location History data through its "Timeline" feature, a depiction of a user's collected Location History points over time. (ECF No. 96-1, at ¶ 5; *see* ECF No. 202, at 79.) According to Google, this permits Google account holders to

[8] Other companies such as Amazon and Apple invariably retain users' location data as well. But Google, whose services function across Apple *and* Android devices (as opposed to Apple Maps for example, which functions only on iPhones), seems to be subject to more geofence requests than other companies.

"choose to keep track of locations they have visited while in possession" of their mobile device. (ECF No. 96-1, at ¶ 4.) Importantly, Location History also supports Google's advertising revenue.[9] For instance, McGriff testified that Location History data serves Google's advertising business by providing "store visit conversions" or "ads measurement" to businesses based on user location. (ECF 201, at 196–97.) Without identifying any individual user, this "store conversion" data can follow a particular ad campaign and identify "how many users who saw a particular ad campaign actually went to one of those stores." (ECF No. 201, at 197.) Google's "radius targeting" also allows—again without identifying any user—"a business to target ads to users that are within a certain distance of that business." (ECF No. 201, at 198.)

Location History is powerful: it has the potential to draw from Global Positioning System ("GPS") information, Bluetooth beacons, cell phone location information from nearby cellular towers, Internet Protocol ("IP") address information, and the signal strength of nearby Wi-Fi networks. According to Agent D'Errico, Location History logs a device's location, on average, every two minutes.[10] Indeed, Location History even allows Google to "estimat[e] . . . where a device is in terms of elevation." (ECF No. 202, at 95.) McGriff testified that this capability helps locate someone in an emergency, or try to "determine if you are on the second [or first] floor of the mall" if the Google Maps directory has launched to help a user navigate indoors. (ECF No. 202, at 95–96.)

---

[9] Using 10K filings from Google's parent company Alphabet, FBI Agent D'Errico noted that Google's advertising revenue constituted 85.4% and 83.9% of its *entire* revenue in 2018 and 2019, respectively.

[10] Defense Expert McInvaille evaluated a sample set of data and found that, for that data, Location History logged a device's location every six minutes. Under McInvaille's estimate, a user's movement is logged 240 times a day. D'Errico's estimate would raise that to 720 times a day. And Google Expert McGriff confirmed that Location History can track a user "hundreds" of times a day. (ECF No. 202, at 159.)

Google stores this data in a repository known as the "Sensorvault" and associates each data point with a unique user account. (ECF No. 201, at 130.) The Sensorvault contains a substantial amount of information. McGriff testified that the Sensorvault assigns each device a unique device ID—as opposed to a personally identifiable Google ID—and receives and stores *all* location history data in the Sensorvault to be used in ads marketing. Google then builds aggregate models within the Sensorvault with data that is transformed so that it no longer looks like user data, and then uses the data to, for instance, assist decision-making in Google Maps. As another example, Google uses this data to depict whether certain locations are busy during particular hours. Both McGriff and Rodriguez declared that, to identify users within the relevant timeframe of a geofence, Google has to compare *all* the data in the Sensorvault in order to identify users within the relevant timeframe of a geofence. (ECF No. 96-1, at ¶ 23 ("Google must search across *all* [Location History] data," and "run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant."); ECF No. 96-2, at ¶ 7 ("Google must conduct the search across *all* [Location History] data.").) Clearly, however, Google can alter the data back to identify users in response to a geofence warrant.

Still, Location history is off by default. A user can initiate, or opt into, Location History either at the "Settings" Level, or when installing applications such as Google Assistant, Google Maps, or Google Photos. Although the specific software pathway each user sees at any given moment can differ based on numerous factors, McGriff acknowledged that it was "possible that a user would have seen the option" to opt into Location History multiple times across multiple apps. (ECF No. 202, at 77–78.) For instance, Google may prompt the user to enable Location

History first in Google Maps, then again when he or she opens Google Photos and Google Assistant for the first time.[11]

Once a user opts into Location History, Google is "always collecting" data and storing *all* of that data in its vast Sensorvault, even "if the person is not doing anything at all with [his or her] phone." (ECF No. 201, at 114–15; *see* ECF No. 201, at 115 ("Once enabled, [Google is] now collecting [the user's] location history all the time.").) Even if a user enables Location History through an application and later deletes that app, Location History will "still collect[]" data on the user because Location History is tied to an individual's Google *account*, not to a *specific app*. (ECF No. 201, at 123–24.) Thus, after a user opts into the service, Location History tracks a user's location across every *app* and every *device* associated with the user's account. Approximately one-third of all active Google users have Location History enabled on their accounts.

In certain circumstances, Google can estimate a device's location down to three meters. Location History cannot, however, pinpoint an individual's location with absolute precision. Instead, Google *estimates* a phone's coordinates. When Google, through Location History, reports a device's estimated location by placing a point on a map, it also depicts around that point a "confidence interval"—a circle of varying sizes—which indicates Google's confidence in its estimation. (ECF No. 201, at 38, 212; ECF No. 202, at 253–54.) The smaller the circle around a phone's estimated location, the more confident Google is in that phone's exact location, and *vice versa*. In general, "Google aims to accurately capture roughly 68 percent of users"

[11] In a highly critical 2018 evaluation of tracking through Location History and Web & App Activity, the Norwegian Consumer Council (funded by the Norwegian government) characterized this as one of an identifiable set of problematic practices, dubbing it "repeated nudging" to encourage a user to enable the app. (Mar. 4–5 Hr'g Def. Ex. 27, at 28.)

within its confidence intervals. (ECF No. 201, at 213.) "[I]n other words, there[is] a 68 percent likelihood that a user is somewhere inside" the confidence interval. (ECF No. 201, at 213.)

ii. Web and App Activity

Web and App Activity collects a wider variety of information than Location History. If a user opts into WAA and has authorized all other requisite device permissions, WAA collects certain data points when a user *affirmatively engages* in certain activities.[12] For example, when a user performs a Google search, Google may, through WAA, keep a record of that search so that it can "automatically suggest[]" that search to the user at a later time. (ECF No. 96-1, at ¶ 16.) Google maintains that WAA allows a user to "experience faster searches and more helpful app and content recommendations." (ECF No. 96-1, at ¶ 16.) "Some of [the data obtained through WAA] can include location information, although the source of the location information will vary depending on the activity, the device, and the user's other settings." (ECF No. 96-1, at ¶ 16.) Location History "and WAA are separate services that store data in separate databases." (ECF No. 96-1, at ¶ 16.) That is, "WAA data is not used to calculate the locations that are stored in [Location History], and completing a search across [Location History] data does not search or draw on WAA data in any way." (ECF No. 96-1, at ¶ 16.)

iii. Google Location Accuracy

Lastly, Google Location Accuracy—only available on Android devices[13]—allows a user's phone to draw in location data from sources other than GPS information. "If a user has the GLA setting on, the Android[device's] location services will use additional inputs, including Wi-Fi access points, mobile networks, and sensors[] to estimate the device's location." (ECF

[12] This stands in contrast to Location History, which constantly and *passively* logs a user's location.

[13] At the time of the robbery, Chatrie used an Android device.

No. 96-1, at ¶ 17.) Thus, "the device 's location information that is sent to and stored in [Location History] . . . may be calculated using not only GPS-sourced data, but also [more detailed] WiFi- or cell-sourced data from the GLA database." (ECF No. 96-1, at ¶ 17.) "In other words, GLA data might be used by the device to calculate a [more precise] location data point that is then stored in [Location History]." (ECF No. 96-1, at ¶ 17.) Like WAA, Google generally stores GLA data separate from Location History information.

Again, as a general matter, Google appears to draw only from Location History to produce records for geofence requests, as WAA and GLA do not collect enough data points to pinpoint "devices within a certain period of time within a certain radius." (ECF No. 202, at 138; *see* ECF No. 201, at 211; ECF No. 96-1, at ¶¶ 20–22.) In keeping with this principle, here, Google only produced to law enforcement information from its Location History database.

b. Enabling Location History

The Court reports its understanding of the software pathways necessary to enable Location History based on two sets of sources. All sources agree that Chatrie enabled his Location History on July 9, 2018. However, even with input from two knowledgeable witnesses, the record as to how users can and do—and how Chatrie in particular could and did—enable Location History is not definitive on this record.

First, Defense Expert Spencer McInvaille testified in Court using a video of a device employing what was likely the same software used by Chatrie's phone to demonstrate how one might activate Location History through the Google account setup or through an app such as Google Maps. (Jan. 21 Hr'g Def. Ex. 4 ("Opt-In Video").) McInvaille also offered a written report explaining how Chatrie may have enabled location history. In that report, McInvaille

reported that Chatrie most likely enabled LH using Google Assistant, and that it was enabled on July 9, 2018.

Second, Google Location History Product Manager Marlo McGriff filed three declarations that explain how Google collects, stores, and turns over Location History data. He also testified in person during the March 4–5 Suppression Hearing. In his second declaration, McGriff concedes that McInvaille's video exhibit depicts largely accurate pathways to enable Location History. But McGriff states that McInvaille's video is incomplete. McGriff notes that "[b]y 2017 at the latest, it was not possible for a user to unable [Location History] solely by tapping on 'YES, I'M IN' as depicted on the final screen in the McInvaille Video." (ECF No. 110-1, at ¶ 7.) Instead, "a user who tapped on 'YES, I'M IN' . . . would be presented with a second opt-in screen" described above. (ECF No. 110-1, at ¶ 7.) McGriff presents the Court with the exact text of the second opt-in screen in his Third Declaration.[14] (ECF No. 147, at ¶¶ 7–8; *see* ECF No. 147, at ¶ 10 ("The text quoted in ¶¶ 7–8 is the same text that [Chatrie] would have seen on July 9, 2018.").

No expert could say *exactly* which software pathway Chatrie would have seen when he enabled Location History, nor could Google determine which app he used to turn the service on. Google does, however, accept that Chatrie would have seen the informational text in Part II.A.3.b.ii ("Through an App") in *some* form.

i. Through Phone Setup

As mentioned, a user must affirmatively enable Location History before Google uses the service to log the user's whereabouts. Google first allows users to enable Location History

[14] McGriff complicated this seemingly straightforward proposition by acknowledging that any "device that has been sitting on a shelf for three years [would use start up language] dated to when it was baked into the device." (ECF No. 202, at 18.)

during the initial Google account setup process. After a new user connects the phone to the internet, agrees to the phone manufacturer's terms and conditions, and inputs the necessary information to create a Google account, the interface displays Google's terms of service. (*See* ECF No. 110-1, at ¶ 5 (acknowledging that the Opt-In Video exhibit was accurate but incomplete).) To move past this screen, the user must scroll through a summary of Google's privacy terms until the user reaches the bottom of the page. This page "does [not] . . . say anything about [L]ocation [H]istory." (ECF No. 81, at 51.) Near the bottom, the screen displays blue text that reads, "MORE OPTIONS," with a downward-facing arrow next to the text. (Opt-In Video 3:00.) If the user taps on "MORE OPTIONS," the interface displays additional information about Google's location services. (ECF No. 81, at 51.) This additional information informs the user that WAA and GLA are enabled by default. Although Location History is *not* enabled by default, the user can opt into it from this screen by checking a box.

ii. Through an App

If a user does not enable Location History while setting up his or her Google account, Google will also prompt the user to turn the service on as soon as he or she sets up an app "that has [Location History]-powered features." (ECF No. 110-1, at ¶ 5; *accord* ECF No. 96-1, at ¶¶ 3–6; ECF No. 201, at 221; ECF No. 202, at 8–9.) Such apps include Google Maps, Google Photos, and Google Assistant. When a user opens one of these apps for the first time, the phone immediately directs the user to a bright blue screen that reads: "Get the most from Google Maps." (Opt-In Video 4:36.) This screen informs the user that "Google needs to periodically store [his or her] location to improve route recommendations, search suggestions, and more." (Opt-In Video 4:36.) Below that, the interface offers the user the option to "LEARN MORE." (Opt-In Video 4:36.) If the user taps "LEARN MORE," the page redirects to "[a]ll of [Google's]

terms and conditions"—but these terms and conditions include no information specifically tailored to location information. (ECF No. 81, at 57.)

Back at the initial blue page, the user can either select "YES, I'M IN" or "SKIP." (Opt-In Video 4:36.) As of July 2018, once the user selects "YES, I'M IN," the interface redirects the user to another page that displays the following text:

> **Location History**
>
> Saves where you go with your devices ∨ [15]
>
> This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

(ECF No. 147, at ¶ 7 (bold in original).) Next to "Location History: Saves where you go with your devices," the interface includes an "expansion arrow," depicted in the above text with a downward-facing caret. (ECF No. 147, at ¶ 8.) If a user "tap[s] on [this] expansion arrow," the interface "present[s the user] with additional information about" Location History. (ECF No. 147, at ¶ 8.) The screen then reads:

[15] Although the testimony is unclear on the matter, prior to 2018, this line appears to have read: "[C]reates a private map of where you go with your signed in devices." (ECF No. 201, at 266.) Google changed this language in response to European regulation.

Location History

Saves where you go with your devices

Location History saves where you go with your devices. To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, like Google Maps or Search.

If you use your device without an internet connection, your data may be saved to your account once you return online.

Not all Google services save this data to your account.

This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google.

This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.

NO THANKS TURN ON

(ECF No. 147, at ¶ 8 (bold in original).) If the user selects "TURN ON"—either in the original screen or this expanded version—Location History is enabled. (ECF No. 147, at ¶ 9.) Importantly, a user need not interface with or employ the expansion arrow to enable Location History. In other words, a user could activate the service without knowing any of the further details of the service as explained in the above expanded version.

As noted, Chatrie enabled Location History on his device on July 9, 2018 at 12:09 a.m. Eastern Standard Time, and he appears to have done so through Google Assistant.

c. "Pausing" and Trying to Delete Location History

After a user opts in, he or she has two mechanisms to manage Google's collection and retention of his or her Location History data: "pausing" the service, or deleting the information it collected.

i. Pausing

As Google Location History Product Manager Marlo McGriff explained, when a user "*pauses*" his or her Location History, it merely "halts the collection of future data;" *it does not delete* information Google has already obtained. (ECF No. 202, at 84.) And deleting an app through which the user enabled Location History will not pause the service.

A user may pause Location History on an Android device in one of three locations. First, the user can pause it "through the settings on any particular app that uses Location History." (ECF No. 202, at 63.) Second, he or she can pause it by navigating "through the device level settings." (ECF No. 202, at 63.) Finally, the user can log into myactivity.google.com and change his or her location settings. For each of these options, "a user [must] actively, intentionally navigate" through each interface. (ECF No. 202, at 64.)

When a user attempts to pause Location History, the device will present a pop-up screen containing text called the "pause copy." (Mar. 4–5 Hr'g Def. Ex. 27, at 23.) The pause copy warns users that pausing Location History will "limit[] functionality of some Google products over time, such as Google Maps and Google Now." (Mar. 4–5 Hr'g Def. Ex. 27, at 23; *accord* ECF No. 202, at 66.) Yet the record suggests that apps such as Google Assistant *will* continue to function with Location History paused. For instance, McInvaille noted that, despite prompts from Google to initiate Location History because apps like Google Assistant "depen[d] on these

settings in order to work correctly," the user does not "need Location History for [Google Assistant] to work." (ECF. No. 201, at 111, 113.)

The pause copy also does not specifically detail how app functionality might be limited. Nor does Google inform users of the fact that the app will, indeed, continue to function without Location History enabled, either when setting up the application or when displaying the pause copy. McGriff confirmed that when a user "pauses" the service, it halts only the collection of future data, and it does not (if a user has opted in) pause other location services such as Web & App Activity. (ECF No. 202, at 84, 90.)

ii. Trying to Delete

In 2018, when Chatrie enabled his Location History, a user had only one option to *delete* his or her Location History: by visiting myactivity.google.com and viewing his or her Timeline. Through the Timeline, a user "can review, edit, or delete [his or] her [Location History data] at will." (ECF No. 96-1, at ¶ 15.) But in response to an article from the Associated Press criticizing Google's acquisition of location data, one Google employee apparently remarked through an email: "The current [User Interface as of August 13, 2018] *feels* like it is designed to make things *possible*, yet *difficult* enough that people won't figure . . . out" how to turn Location History off.[16] (Mar. 4–5 Hr'g Def. Ex. 30, at 6 (emphasis added).) Whether the substance of this remark is true or not, the sentiment it expresses is certainly not inconsistent with the record before the Court.

[16] On May 11, 2018, two Senators launched an investigation into Google's acquisition of location data. During the March 4–5 Suppression Hearing, Chatrie tried to suggest that this investigation—in conjunction with a critical article from news website Quartz—*caused* Google to issue an update to its privacy policy on May 25, 2018. Google's expert McGriff testified credibly, however, that the investigation and policy changes were unrelated, because "there[was] no way Google updated its privacy policy in two weeks." (ECF No. 201, at 259.)

The effort to clarify this interface obviously is ongoing at Google.[17] In May 2019, McGriff formally heralded the "autodelete" controls that made it easier for users to manage their data. (*See* Mar. 4–5 Hr'g Def. Ex. 46.) And in December of 2019, McGriff introduced, on behalf of Google, "Incognito mode" and "Bulk delete in Timeline." (*See* Mar. 4–5 Hr'g Def. Ex. 47.)

d. Google's Process in Answering a Geofence Warrant

Geofence warrants represent "a novel but rapidly growing [investigatory] technique." (ECF No. 59-1, at 8.) When law enforcement seeks a geofence warrant from Google, it (1) identifies a geographic area (also known as the "geofence," often a circle with a specified radius), (2) identifies a certain span of time, and (3) requests Location History data for all users who were within that area during that time. (*See* ECF No. 96-2, at ¶ 4.) The requested time windows for these warrants "might span a few minutes or a few hours." (ECF No. 96-2, at ¶ 4.)

In recent years, the number of geofence warrants received by Google has increased exponentially. Google received its first in 2016. After that, Google "observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and the

[17] Since 2018, Google has added another feature to increase user control over Location History data. It now allows a user to set an "auto delete function" that limits how long Location History information remains with Google. (Mar. 4–5 Hr'g Def. Ex. 46, at 2.) The auto delete function now enables a user to "[c]hoose a time limit" for how long he or she wants Google to save activity data and "any data older than that will be automatically deleted from [the] account on an ongoing basis." (Mar. 4–5 Hr'g Def. Ex. 46, at 2.) McGriff testified that Google has also now developed a practice whereby Google sends monthly or annual emails about how to change settings. Google has no record that these emails were ever sent to Chatrie.

Still, concern about the user interface seemed to persist over time. Chatrie presented what purported to be emails from Google employees (garnered for other litigation) noting the confusing nature of various location products. One, in April 2019, reads: "Speaking as a user, WTF? More specifically I **thought** I had location tracking turned off on my phone. However the location toggle in the quick settings was on. So our messaging around this is enough to confuse a privacy focused Google-[software engineer]. That's not good." (Mar. 4–5 Hr'g Def. Ex. 37, at 5). The Norwegian report called this phenomenon "[d]eceptive click-flow." (Mar. 4–5 Hr'g Def. Ex. 27, at 27).

rate . . . increased over 500% from 2018 to 2019." (ECF No. 59-1, at 8.) In 2019, Google received "around 9,000 total geofence requests."[18] And Google now reports that geofence warrants comprise more than twenty-five percent of *all* warrants it receives in the United States. Google, *Supplemental Information on Geofence Warrants in the United States* (last visited Mar. 1, 2022), https://bit.ly/3o7Znqc.

Google began to take issue with certain early geofence warrants because the requests were too broad. As related by Legal Investigations Specialist Rodriguez, the warrants "sought [Location History] data that would identify *all* Google users who were in a geographical area in a given time frame." (ECF No. 96-2, at ¶ 5 (emphasis added).) Thus, in 2018, Google held both internal discussions with its counsel and external discussions with law enforcement agencies, including the Computer Crime and Intellectual Property Section of the United States Department of Justice ("CCIPS"), to develop internal procedures on how to respond to geofence warrants. "To ensure privacy protections for Google users, . . . Google instituted a policy of objecting to any warrant that failed to include de[-]identification and narrowing measures." (ECF No. 96-2, at ¶ 5.) Seemingly developed as a result of Google's collaboration with CCIPS, this de-identification and narrowing "protocol typically . . . entails a three-step process." (ECF No. 96-2, at ¶ 5; *see* ECF No. 202, at 553.) As noted earlier, the Court draws its understanding of this process from an amalgam of in-person testimony and a declaration submitted by current Google Tooling and Programs Lead and former Legal Specialist Sarah Rodriguez.

[18] To clarify, a geofence *request* is not identical to a geofence *warrant*. "[I]n some cases, law enforcement is[not] aware that [it] need[s] to submit a warrant" to obtain Location History. (ECF No. 202, at 173.) Google still considers this communication from law enforcement a "geofence request," even when not accompanied by a warrant. (ECF No. 202, at 173.)

i. Step 1

First, at Step 1, law enforcement receives a warrant "compelling Google to disclose a *de-identified* list of all Google user[s]" whose Location History data indicates were within the geofence during a specified timeframe. (ECF No. 96-2, at ¶ 6 (emphasis added).) In response to the warrant, Google must "search . . . *all* [Location History] data to identify users" whose devices were present within the geofence during the defined timeframe. (ECF No. 96-2, at ¶ 7; ECF No. 96-1, at ¶ 23.) "Google does not know which users may have . . . saved [Location History] data before conducting th[is] search." (ECF No. 96-2, at ¶ 7.)

Rodriguez stated that, as part of this first step, Google provides the Government with responsive user records identified in the Sensorvault. Google deems a record "responsive" if a user's estimated location (*i.e.*, the stored coordinates of the phone in Location History) falls within the boundaries of the geofence. (ECF No. 96-1, at ¶ 25.) Rodriguez confirmed that, for every device whose "stored latitude/longitude coordinates fall within the radius described in the warrant," Google turns over a "'production version' of the [users'] data." (ECF No. 96-2, at ¶ 8.) This production version "includes a [de-identified] device number,[19] the latitude/longitude coordinates and timestamp of the stored [Location History] information, the map's [confidence

---

[19] When responding to geofence warrants, Google:

> de[-]identifies the data produced to the [G]overnment at this [first] step by removing the [user's distinct] Google Account ID . . . , leaving only a device number that is used only in the Location History database. This device number is only used for distinguishing devices reporting [Location History] to a user's account . . .

(ECF No. 96-2, at ¶ 9.) Unlike a Google Account ID, a Location History device number does not by itself identify which account is associated with certain location points. However, as discussed in Part II.A.6.b ("The Three Paths Video"), *infra*, piecing together an "anonymous" user's location data could reveal that user's identity.

interval], and the source of the stored [Location History]," (*i.e.*, "whether the location was generated via Wi-Fi, GPS, or a cell tower"). (ECF No. 96-2, at ¶ 8.)

According to Rodriguez, the sizes and timeframes of geofences "vary considerably from one request to another." (ECF No. 96-2, at ¶ 8.) Because Google produces *all* location points captured within the geofence over the timeframe, "[t]he volume of data produced at [Step 1] depends on the size and nature of the geographic area and length of time covered by the geofence request." (ECF No. 96-2, at ¶ 8.) Google does not impose specific, objective restraints on the size of the geofence, the length of the relevant timeframe, or the number of users for which it will produce data.

Indeed, Google places significant discretion on the LIS employee who initially reviews a particular geofence warrant. This "specialist" will first process and review the warrant. (ECF No. 202, at 178–79.) If the specialist believes the warrant "needs further review"—for example, if the geofence seems too large or the timeframe too long—he or she may first "engage with [the requesting] law enforcement officer to collect more information about the investigation." (ECF No. 202, at 179, 182.) From there, the specialist will "consult with [Google's] legal counsel." (ECF No. 202, at 179.) If Google's counsel objects to the warrant, Google may have a "conversation" with law enforcement to alleviate Google's concerns, or it may "require law enforcement to obtain an amended or a newly-issued warrant that addresses the issue." (ECF No. 202, at 187.) Assuming law enforcement eventually assuages Google's concerns with the warrant, Google then provides the Government with the de-identified geofence data.

ii. Step 2

Second, according to Rodriguez, at Step 2, the Government "reviews the de[-]identified [data] to determine the [Sensorvault] device numbers of interest." (ECF No. 96-1, at ¶ 10.) If

law enforcement needs "additional de[-]identified location information for a [certain] device" to "determine whether that device is actually relevant to the investigation," law enforcement, at this step, "can compel Google to provide additional . . . location coordinates *beyond* the time and geographic scope of the original request."[20] (ECF No. 96-2, at ¶ 10 (emphasis added).) These additional location points "can assist law enforcement in eliminating devices" from the investigation that were, for example, "not in the target location for enough time to be of interest, [or] were moving through the target location in a manner inconsistent with other evidence."[21] (ECF No. 96-2, at ¶ 11.) Notably, Google imposes "no geographical limits" on this Step 2 data. (ECF No. 202, at 184.) Thus, if a user's location fell within the geofence at Step 1, law enforcement can obtain *all* location points for identified users over an expanded timeframe at Step 2. This means that, at Step 2, no geographic barrier confines the information searched.

Google does, however, typically require law enforcement to narrow the number of users for which it requests Step 2 data so that the Government cannot not simply seek geographically unrestricted data for *all* users within the geofence. Google has no firm policy as to precisely *when* a Step 2 request is sufficiently narrow. But if law enforcement requests "a lower number of devices from St[ep] 1 to St[ep] 2," this, to some extent, demonstrates to Google that law enforcement has tailored the data it seeks. (ECF No. 202, at 190.) Again, assuming Google has no further objections to law enforcement's Step 2 request, Google provides law enforcement with de-identified but geographically unrestricted data.

---

[20] At Step 2, for law enforcement to expand the timeframe from which to obtain Location History data, Google generally requires that the warrant explicitly expand that timeframe *in the warrant's text*. Otherwise, Google will object to that request.

[21] If law enforcement requests this additional data, it must typically do so within sixty days.

iii. Step 3

Finally, at Step 3, drawing from the de-identified data Google has produced so far, "the [G]overnment can compel Google . . . to provide *account-identifying information*" for the users "the [G]overnment determines are relevant to the investigation." (ECF No. 96-2, at ¶ 12 (emphasis added).)[22] This "account-identifying information" includes the name and email address associated with the account. (ECF No. 96-2, at ¶ 12; ECF No. 202, at 192.) Google seems to prefer that law enforcement request Step 3 data on fewer users than requested in Step 2, although it is "[p]ossibl[e]" that Google would approve a Step 3 request that is not narrowed after Step 2 at all. (ECF No. 202, at 194.)

4. The Instant Geofence Warrant and Its Justifications

a. Det. Hylton's Investigation[23]

When Det. Hylton responded to the scene of the bank robbery on May 20, 2019, he "interviewed witnesses" and "reviewed surveillance camera video from . . . the Call Federal Credit Union Bank." (ECF No. 202, at 330.) Through this initial investigation, he "learned that [the] suspect had come from the southwestern corner of the Journey Christian Church [the 'Church'], . . . a building adjacent and to the east of the Call Federal Credit Union, at approximately 4:50 in the afternoon." (ECF No. 202, at 330–31.) He also learned of the core

[22] Law enforcement has sixty days from the time Google turns over Step 2 data to request Step 3 information.

[23] Although the subsequent warrants evaluated in a separate Opinion, explain officers' investigatory efforts to identify a suspect beyond reviewing security camera footage, the Geofence Warrant contains no information about those efforts. Because the Geofence Warrant does not expressly incorporate these subsequent warrants—and indeed, it could not have because officers obtained them after drafting the Geofence Warrant—the Court will consider only the following facts in its analysis. *See United States v. Hurwitz*, 459 F.3d 463, 470 (4th Cir. 2006) (requiring that a warrant either incorporate a supporting document by reference or attach the document to warrant itself in order for a court to read the document alongside the warrant).

facts that underlie this case—that the suspect walked into the Bank wearing a fisherman's hat and traffic vest, presented the teller with a note demanding $100,000, forced the manager at gunpoint to open the Bank's vault, took $195,000, and may have left in a blue Buick Lacrosse. Critically, through security footage, Det. Hylton observed that when the suspect first walked into Bank, he was "holding what appeared to be . . . a cell phone to the side of his face." (ECF No. 202, at 331.) To Det. Hylton, this use of a phone suggested "that [the suspect] could have possibly been speaking with a coconspirator." (ECF No. 202, at 333.)

After Det. Hylton completed his on-site investigation, he pursued at least two other leads. First, a purportedly estranged romantic partner called the police and told them that she "kn[e]w who did th[e] robbery," and that the suspect was her "ex-boyfriend." (ECF No. 202, at 334.) Law enforcement found this ex-boyfriend, interviewed him, examined his cell phone, and ultimately determined that he was not the suspect. Next, an employee at another branch of the Bank alerted the police about an individual who drove a blue Buick Lacrosse and wore a traffic vest. Det. Hylton ultimately determined that this individual was likewise not the suspect.

Having unearthed no further leads from his investigation, Det. Hylton then turned to geofence technology. He had sought three other geofence warrants in the past. Before seeking those warrants, he had consulted with prosecutors, who approved them. Magistrates—including one federal magistrate judge—approved all three as well. Those warrants were, according to Det. Hylton, "mostly similar" to the one at bar. (ECF No. 202, at 328; *compare* Mar. 4–5 Hr'g Def. Ex. 18 ("Prior Federal Geofence Warrant") *and* Mar. 4–5 Hr'g Def. Ex. 19 ("Prior State Geofence Warrant") *with* ECF No. 54-1.) Indeed, all but one adopted a roughly 150-meter radius, although a "few of them had more locations because [there were] more robberies to

investigate." (ECF No. 202, at 328; *see* Prior Federal Geofence Warrant; Prior State Geofence Warrant.)

On June 14, 2019, roughly three weeks after the robbery, Det. Hylton applied for and obtained the instant Geofence Warrant from Chesterfield County Magistrate David Bishop.

b. Magistrate Bishop

Chatrie contests the sufficiency of Magistrate Bishop's qualifications. Although the Court will address that issue more fully later in this Opinion, the Court briefly notes that Chesterfield County Magistrate "David Bishop graduated from Pensacola Christian College with a Bachelor's of Science in Criminal Justice in May 2016."[24] (ECF No. 156, at 1.) Around two years later, on June 12, 2018, the Executive Secretary of the Supreme Court of Virginia appointed Bishop as a magistrate. Magistrate Bishop completed his statutorily required probationary period on March 12, 2019. He was released for service on October 24, 2018.

Three months after Magistrate Bishop finished his probationary period, Det. Hylton presented Magistrate Bishop with the instant Geofence Warrant. When Magistrate Bishop reviewed the Warrant, he asked no questions of Det. Hylton, nor did he "seek to modify anything in the affidavit." (ECF No. 202, at 362.) Based on Det. Hylton's understanding, Magistrate Bishop simply "read [the Warrant] and signed it."[25] (ECF No. 202, at 362.) The record suggests that this was the first geofence warrant Magistrate Bishop had signed.

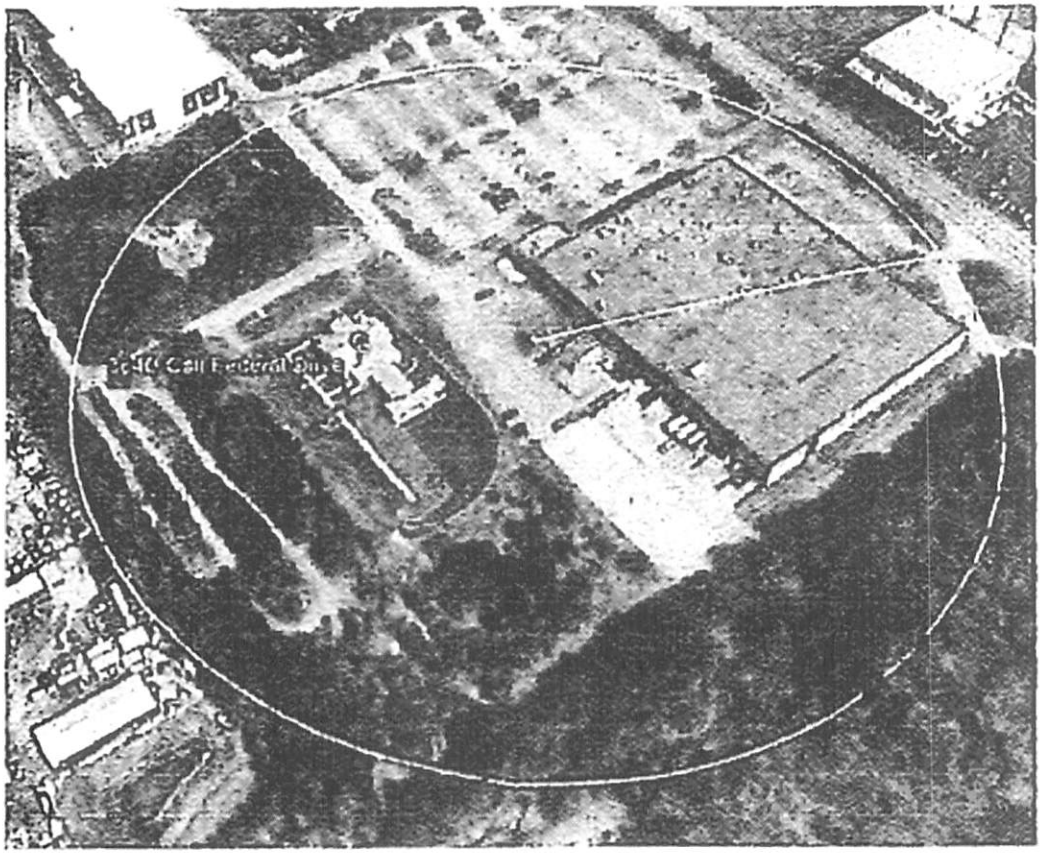
---

[24] The Virginia Code imposes one educational requirement on the Commonwealth's magistrates: they must possess a bachelor's degree "from an accredited institution of higher education." Va. Code § 19.2-37. The Code does not further define what qualifies as an "accredited institution" for the purpose of magistrates. Chatrie disputes whether Magistrate Bishop's alma mater, Pensacola Christian College, is sufficiently "accredited" under the Virginia Code. (ECF No. 135, at 6–9.) The Court will speak to this later in the Opinion.

[25] Det. Hylton did note, however, that because Magistrate Bishop did not read the Warrant in front of him, Magistrate Bishop "*could* have consulted with someone" about it. (ECF No. 202, at 362 (emphasis added).)

c. The Instant Geofence Warrant

The Warrant drew a geofence with a 150-meter radius—with a *diameter* of 300 meters, longer than three football fields—in an urban environment which included the Bank and the nearby Journey Christian Church.[26] All told, the geofence encompassed 17.5 acres. The eastern side of the geofence abutted but did not include Price Club Boulevard. The southern side encompassed a wooded area behind the Bank. The northern side encircled the Church's parking lot, and the western side captured a wooded area to the west of the Bank. The Warrant included the following photograph of the area with the geofence superimposed over it:



[26] Thus, the total area of the geofence is 70,686 square meters—about three and a half times the *footprint* of a New York city block. Michael Kolomatsky, *How Big Is an Acre, Anyway?* N.Y. Times (July 26, 2018), https://nyti.ms/345CjS7. Of course, this portion of suburban Richmond, Virginia does not have the density (or height) comparable to that of seven New York City blocks.

The Warrant sought location data for every device present within the geofence from 4:20 p.m. to 5:20 p.m. on the day of the robbery. In keeping with Google's established approach, the Geofence Warrant described a three-step process by which law enforcement would "attempt to narrow down" the list of users for which the Government would obtain the most invasive information. (ECF No. 54-1, at 4.)

At Step 1, "Google w[ould] provide 'anonymized information' regarding the Accounts that are associated with a device that was inside the described geographical area" from 4:20 p.m. to 5:20 p.m. (ECF No. 54-1, at 4.) At Step 2, "Law enforcement w[ould] return a list [of accounts] that they ha[d] attempted to narrow down." (ECF No. 54-1, at 4.) Google would then "produce contextual data points with points of travel outside of the geographical area." (ECF No. 54-1, at 4.) During Step 2, the warrant expanded the timeframe to include thirty minutes before and thirty minutes after the initial hour-long window, so that the Step 2 window was two hours long in total. (ECF No. 54-1, at 4.) Finally, at Step 3, after Government review, Google would "provide identifying account information/CSI[27] for the accounts requested" by law enforcement. (ECF No. 54-1, at 4–5.)

In explaining why "Google [should] provide Geo[f]encing data," Det. Hylton noted in the warrant's accompanying affidavit that:

---

[27] The warrant included in the definition of "identifying account information/CSI" the following:

> user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used to set up the account, verify the account or to receive assistance with the account, and Google Voice phones numbers associated with the account.

(ECF No. 54-1, at 4.)

> when people act in concert with one another to commit a crime, they frequently utilize cellular telephones and other such electronic devices, to communicate with each other through WiFi, Bluetooth, GPS, voice calls, text messages, social media accounts, applications, emails, and/or cell towers in the area of the [crime].

(ECF No. 54-1, at 6.) Specifically, he noted that when reviewing the Bank's surveillance footage, he observed that the perpetrator "had a cell phone in his right hand and appeared to be speaking with someone on the device." (ECF No. 54-1, at 6.) He further explained that:

> Google has . . . developed a proprietary operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.
>
> Based on [his] training and experience, [he has learned] that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled.

ECF No. 54-1, at 7.) Therefore, he explained, "the requested data/information would have been captured by Google during the requested time." (ECF No. 54-1, at 6.) Det. Hylton noted several ways law enforcement could use this information. For example, "location data . . . may tend to identify potential witnesses and/or suspects." (ECF No. 54-1, at 7.) In turn, this geographic and timeline information may tend to "inculpat[e] or exculpate[e] persons of interest." (ECF No. 54-1, at 7.)

Inexplicably, on June 19, 2019—*the day before he sent the Warrant to Google*—Det. Hylton submitted his return for the Warrant to the Chesterfield County Circuit Court. A search warrant return "notifies the Court when [an officer] *execute*[*s*] a search warrant," and the officer "report[s] back to the Court what items [he or she] gathered during the search." (ECF No. 202, at 366–68 (emphasis added).) In the return, he stated that he had executed the warrant on June 14, 2019. Yet he had not yet sent the Warrant to Google. Moreover, in describing the items

already seized under the Warrant—again, he had not yet executed it—Det. Hylton wrote for what would be a sizable amount of precise location information on at least nineteen device users: "Data." (Mar. 4–5 Hr'g Gov't Ex. 2, at 9; *see* ECF No. 202, at 367, 369); *see also United States v. Williams*, 592 F.3d 511, 520 (4th Cir. 2010) ("While the [Fourth Amendment's] protection cannot demand perfection, any tolerance of imperfection does not give officers free reign to ransack and take what they like." (citation and quotation marks omitted)).

5. Google Receives the Geofence Warrant

The next day, on June 20, 2019, Det. Hylton sent Google the Warrant that Magistrate Bishop had approved. Pursuant to Step 1, Google produced anonymized Location History data for all accounts associated with phones present within the geofence from 4:20 p.m. to 5:20 p.m.—nineteen users in total.[28] Associated with these nineteen users were 210 individual location points, along with the confidence interval for each point. In this case, law enforcement ran this information through a program to produce a visual representation of the data. *See* Part II.A.6.a, *infra*.

A few days after Google provided him the Step 1 information, Det. Hylton emailed Google. The record then strongly suggests that he did not "attempt to narrow down" the list of devices for which he requested further data. In contravention to Google's policy, and without consulting Magistrate Bishop, Det. Hylton requested "additional location data" (Step 2 data) *and* "subscriber information" (Step 3 data) "for *all* 19 device numbers produced in [S]tep 1." (ECF

[28] Google provides this information in a table, sorted into seven columns: "Device ID," "Date," "Time," "Latitude," "Longitude," "Source," and "Maps [Confidence Interval]." (*See, e.g.*, Mar. 4–5 Hr'g Def. Ex. 3, at 7.) Google LIS Rodriguez testified that the Device ID is not an identifier for "any other specific Google account." (ECF No. 202, at 176.) It is not cross-referenced by Google outside of Location History, but if an individual device were responsive to two different geofence warrants, the ID would be the same in both. Law enforcement does not return this information to Google nor, in this case, did it return the data to the Chesterfield County Court.

No. 48-1, at 1; *accord* ECF No. 96-2, at ¶ 15; ECF No. 202, at 195, 345.) He noted that, because "the sought Google devices [were] fairly low in number," he requested Step 2 and 3 data for *all* nineteen users "in an effort to rule out possible co-conspirators." (ECF No. 48-1, at 1; *see* ECF No. 202, at 195.) He admitted, however, that "device numbers 1–9 may fit the more likely profile of [the] parties involved." (ECF No. 48-1.) Six days after sending the email, Det. Hylton called Google and left two voicemails seeking a response.

A Google specialist then called Det. Hylton. As described by Rodriguez, the LIS "explained the issues" with Det. Hylton's request—namely, that the request "did not appear to follow the three sequential steps or the narrowing required by the search warrant." (ECF No. 96-2, at ¶ 16; *see* Mar. 4–5 Hr'g Tr. 189, 197.) "Det. Hylton asked . . . what information would be produced in [S]tep 2 and . . . [S]tep 3." (ECF No. 96-2, at ¶ 16.) The Google specialist explained the nature of the data to be turned over during these steps and emphasized to Det. Hylton "the importance of [S]tep 2 in narrowing." (ECF No. 96-2, at ¶ 16; *see* ECF No. 202, at 197.) The specialist, however, does not appear to have provided Det. Hylton with any "specific directive[s] . . . about how much [Det. Hylton] had to narrow" his request. (ECF No. 202, at 197.) On July 9, 2019, Det. Hylton emailed Google, requesting Step 2 data on the *nine* users identified in his prior email. Google then provided him that information in the same format as Step 1 data had been returned. It does not appear that Det. Hylton explained to Google precisely why he requested Step 2 data for these nine particular accounts. Neither Det. Hylton nor Google consulted with a magistrate or judge before Google disclosed this data.

"On or about July 10, 2019, and July 11, 2019, Google received emails from [Det.] Hylton requesting [Step 3] information . . . on [three] device numbers." (ECF No. 96-2, at ¶ 19.) Google provided him with this information—"the account subscriber information associated with

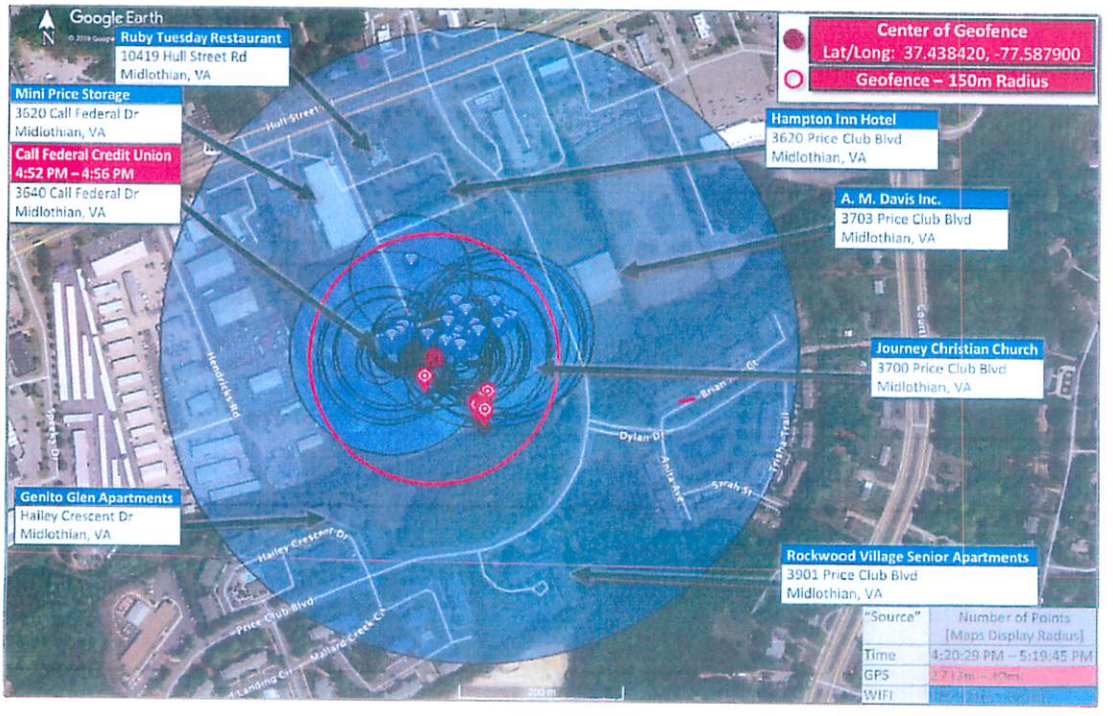
the 3 device numbers"—on July 11. (ECF No. 96-2, at ¶ 20.) Again, it is not apparent from the record whether Det. Hylton demonstrated to Google why he requested Step 3 data for these three accounts, nor did he seek the magistrate's approval before obtaining the data.

Finally, "[o]n or about July 12, 2019," Det. Hylton emailed Google "requesting *additional* device or phone number information that could be associated with one of the accounts" for which Google had produced Step 3 data. (ECF No. 96-2, at ¶ 21 (emphasis added).) This would have been an unauthorized Step 4. A Legal Investigations Specialist called Det. Hylton, that day and told him that "no further information was produced under" the Geofence Warrant. (ECF No. 96-2, at ¶ 21.)

6. Data Derived from the Warrant

a. Law Enforcement's Demonstrative

Upon receipt of the geofence data, law enforcement "imported [the Step 1 information] into mapping software" so that law enforcement could visualize the data points. (Mar. 4–5 Hr'g Gov. Ex. 1, at 15.) That program rendered the following depiction:



The visualization, created by Agent D'Errico, plots each point's confidence interval—the area in which Google is 68 percent confident a given individual is located—with a blue shaded circle.

Here, the largest confidence interval for a user located within the geofence had a radius of roughly 387 meters (longer than four football fields)—more than twice as large as the original geofence.[29] Thus, the Geofence Warrant *could* have captured the location of someone who was hundreds of feet outside the geofence. Within this confidence interval—in addition to the Bank and the Church—are several buildings (with an unknown number of floors), including a Ruby Tuesday restaurant, a Hampton Inn Hotel, several units of the Genito Glen apartment complex, a self-storage business, a senior living facility, two busy streets (Hull Street and Price Club Boulevard), and what appear to be several residences near the southeast edge of the confidence interval. Near the time of the robbery, the individual whose account produced this large confidence interval could have been present at any of these locations instead of within the geofence.

Indeed, given that Google returns locations via these estimated location points, both McInvaille and D'Errico confirmed geofences can return both false positives (someone who is not in the geofence reported as being there) and false negatives (someone in the geofence not

[29] The Court acknowledges that as a matter of fact, it is unlikely that this user would have been located far outside the geofence. As FBI Agent D'Errico testified during the March 4–5 Suppression Hearing, this user first reported a location point within the geofence with a confidence interval of around 84 meters. The next location point, reported only thirty seconds later, was the point with the 387-meter confidence interval—but the user's reported location was in exactly the same spot as the prior point. It is thus unlikely that the user would have traveled from an area in or near the geofence to a location significantly outside of it within thirty seconds. FBI Agent D'Errico did note, however, that these location points were "indicative . . . that the device [was] moving," and that "for some reason, . . . a new center coordinate was not obtained by that phone." (ECF No. 202, at 255.) Nevertheless, the notion that geofences *can* capture information from users who are not even in the vicinity of the relevant area troubles the Court and evinces how broad a sweep these warrants may have.

reported). Chatrie created a video based on the returns of this geofence warrant suggesting that a false positive was returned here.

b. The Three Paths Video

Chatrie's video depicting the movement of three phones was based on the data obtained through the Warrant at Step 2. At the March 4–5 Suppression Hearing, Chatrie introduced a video that plotted the locations of three anonymous individuals whose location data Google turned over at Step 2— "Mr. Blue," "Mr. Green," and "Ms. Yellow." (ECF No. 201, at 63, 67; *see* Mar. 4–5 Hr'g Def. Ex. 5 ("Three Paths Video").)

At the beginning of the two-hour, geographically unlimited, window for which the Government requested Step 2 location data, a cluster of location points for Mr. Blue appeared at a nearby apartment complex. At 4:34 p.m., Mr. Blue seemed to leave the apartment complex, and at 4:35 p.m., Mr. Blue's location estimate appeared inside the geofence, roughly seventeen minutes before the robbery occurred. However, at 4:36 p.m.—twenty-seven seconds later—Mr. Blue appeared outside the geofence on Price Club Boulevard, and by 4:37 p.m., Mr. Blue appeared to be driving down Hull Street. Mr. Blue then drove south and stopped at another residence—clustering location data for five minutes—and eventually drove back toward the original apartment complex, where he remained for the rest of the two-hour window. Because Mr. Blue appeared within the geofence for such a brief period of time—and because he appeared within the fence just as he appeared to drive on a nearby street—Defense Expert McInvaille testified that Mr. Blue may have been a "false positive"—he may not have actually stepped foot within the geofence. (ECF No. 201, at 43–44, 65.)

Mr. Green's location points initially clustered at a hospital for a period of about thirty-five minutes. Eventually, Mr. Green drove south along Old Courthouse Road, ultimately

appearing inside the geofence at 4:41 p.m. Around two minutes later—and nine minutes before the robbery—Mr. Green's estimated location appeared in a residential neighborhood, clustering around one home for the remainder of the two-hour window.

Finally, Ms. Yellow clustered location points at a house from 3:51 p.m. to 4:11 p.m. At 4:18 p.m., she clustered several points near a school, and by 4:26 p.m., she appeared to drive toward the Bank. At 4:31 p.m., she first appeared in the geofence, her location estimate surfacing inside the Bank. She reported two more location points inside the Bank, and by 4:36—eighteen minutes before the robbery—appeared to be driving away from the Bank. She drove south, arrived at the house from which she started, and remained there for the rest of the two-hour window.

Defense Expert McInvaille testified that he was able to access publicly available information such as tax records related to the homes in which Mr. Blue, Mr. Green, and Ms. Yellow appeared to spend significant time. He explained that these records, in conjunction with other publicly available information such as social media accounts, would have allowed him to determine these individuals' likely identities with only a few data points. Law enforcement would, of course, have similar or enhanced research capabilities to identify users based on these "de-identified" location points.

* * *

Ultimately, the Step 3 information law enforcement obtained led the authorities to Chatrie.

B. Procedural History

On September 17, 2019, a grand jury indicted Chatrie on two counts: (1) Forced Accompaniment During Armed Credit Union Robbery, in violation of 18 U.S.C. §§ 2113(a), (d),

and (e); and, (2) Using, Carrying, or Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A). The police issued a warrant, and a magistrate judge signed a Petition and Order for Writ of Habeas Corpus ad Prosequendum ordering that Chatrie, then an inmate at Riverside Regional Jail, appear in the United States District Court for the Eastern District of Virginia to answer for the charges.

On October 1, 2019, Chatrie appeared before the magistrate judge and waived his right to a detention hearing. The magistrate judge ordered Chatrie detained pending trial. On that same day, Chatrie appeared for an arraignment and pleaded not guilty to the charged offenses.

On October 29, 2019, Chatrie filed the instant Geofence Motion to Suppress. (ECF No. 29.) The United States responded, (ECF No. 41), and Chatrie replied, (ECF No. 48). On December 23, 2019, the Court granted Google leave to file an amicus brief. (ECF No. 73.) In response to Chatrie's Federal Rule of Civil Procedure 17(c) subpoenas, Google also filed a total of four declarations by two Google employees: three by Marlo McGriff, and (2) one by Sarah Rodriguez. (ECF Nos. 96-1, 96-2, 110-1,[30] 147.)

On November 9, 2020, around one week before the scheduled Suppression Hearing, Google filed a Motion for Leave to Present Remote Testimony. On November 11, 2020, Chatrie responded in opposition. In this response, Chatrie argued that "[i]n person testimony from the Google employees [was] critical to the Court's resolution of Mr. Chatrie's geofence warrant," and that "Google's continued intrusion into this case warrants a finding from this Court that the

[30] On June 17, 2020, Google sought leave to file a Supplemental Declaration of Marlo McGriff (the "Motion for Leave"). The Court granted the Motion for Leave over Chatrie's objection. Given the close proximity in time, the Court continued the then-scheduled July 2, 2020 geofence hearing. The Court found that "the ends of justice [were] best served by granting a short continuance" because "the Geofence Motion to Suppress presents substantial issues of first impression that require the Court to consider a full and accurate record concerning the technology at issue." (ECF No. 115, at 4.) The Court continued the hearing to November 17, 2020.

Google witnesses are hostile/adverse witnesses." (ECF No. 166, at 1, 6.) After the Court held a status conference on the Motion for Leave to Present Remote Testimony, Chatrie filed a Motion to Continue the November 17, 2020 hearing, seeking to continue the hearing to a time when Google would be able to attend in person. On December 18, 2020, the Court granted Chatrie's Motion to Continue and scheduled the Suppression Hearing for March 4, 2021.

Considering the novel and complex questions of law at issue, the Court allowed the parties to provide supplemental briefing on discovery provided by Google and the March 4–5, 2021 Suppression Hearing. Among others, witnesses from Google—McGriff and Rodriguez—provided the Court with a relatively exhaustive picture of Google's typical response to geofence warrants. Now, after careful consideration of the issues and with the aid of the parties' thorough briefing, the Court concludes that, although this warrant is invalid for lack of particularized probable cause, the Court cannot suppress the resulting evidence because the *Leon* good faith exception applies.

III. Analysis

Chatrie seeks to suppress evidence obtained from the June 14, 2019 Geofence Warrant that covered 70,686 square meters of land around the Bank, located in a busy part of the Richmond metro area. Despite the Court's concerns about the validity of this warrant and the adoption of unsupervised geofence warrants more broadly, the Court will deny Chatrie's Motion to Suppress because the officers sought the warrant in good faith.

A. The Court Will Briefly Address Fourth Amendment Standing

Because the Court will independently deny Chatrie's motion to suppress by considering the validity of the Geofence Warrant, the Court "need not wade into the murky waters of standing," *i.e.*, whether Chatrie has a reasonable expectation of privacy in the data sought by the

warrant. *United States v. James*, No. 18cr216, 2018 WL 6566000, at *4 (D. Minn. Nov. 26, 2018); *see Byrd v. United States*, 138 S. Ct. 1518, 1530 (2018) (Fourth Amendment standing "is not a jurisdictional question and hence need not be addressed before addressing other aspects of the merits of a Fourth Amendment claim.").

Nonetheless, the Court notes its deep concern (underlying both Fourth Amendment standing, and the third-party doctrine discussed below) that current Fourth Amendment doctrine may be materially lagging behind technological innovations. As Fourth Amendment law develops in a slow drip, "technology [continues to] enhance[] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes." *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018). Relevant here, although *law enforcement* limited the warrant's window to two hours, Google—despite efforts to constrain law enforcement access to its data—retains constant, near-exact location information for each user who opts in. *See* Part II.A.3.a, *supra*. The Government thus has an almost unlimited pool from which to seek location data, and "'[w]hoever the suspect turns out to be,' they have 'effectively been tailed'" since they enabled Location History. *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (en banc) (quoting *Carpenter*, 138 S. Ct. at 2218).

Indeed, the "'retrospective quality of [geofence] data' enables police to 'retrace a person's whereabouts,'" and "[p]olice need not even know in advance whether they want to follow a particular individual, or when." *Id.* at 342 (quoting *Carpenter*, 138 S. Ct. at 2218). Until recently, the ease with which law enforcement might access such precise and essentially real-time location data was unimaginable. And it is this expansive, detailed, and retrospective nature of Google location data that is unlike, for example, surveillance footage, and that perhaps

causes such data to "cross[] the line from merely augmenting [law enforcement's investigative capabilities] to impermissibly enhancing" them. *Id.* at 341.

What is more, the Court is disturbed that individuals other than criminal defendants caught within expansive geofences may have no functional way to assert their own privacy rights. Consider, for example, a geofence encompassing a bank, a church, a nearby residence, and a hotel. Ordinarily, a criminal perpetrator would not have a reasonable expectation of privacy in his or her activities within or outside the publicly accessible bank. *See United States v. Knotts*, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). He or she thus may not be able to establish Fourth Amendment standing to challenge a time-limited acquisition of his location data at the bank.

But the individual in his or her residence likely *would* have a heightened expectation of privacy. *Silverman v. United States*, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a [person] to retreat into his [or her] own home and there be free form unreasonable government intrusion."). Yet because that individual would not have been alerted that law enforcement obtained his or her private location information, and because the criminal defendant could not assert that individual's privacy rights in his or her criminal case, *United States v. Rumley*, 588 F.3d 202, 206 n.2 (4th Cir. 2009), that innocent individual would seemingly have no realistic method to assert his or her own privacy rights tangled within the warrant. Geofence warrants thus present the marked potential to implicate a "right without a remedy." *Hawkins v. Barney's Lessee*, 30 U.S. 457, 463 (1831) ("There can be no right without a remedy to secure it.").

As this Court sees it, analysis of geofences does not fit neatly within the Supreme Court's existing "reasonable expectation of privacy" doctrine as it relates to technology. That run of cases primarily deals with *deep*, but perhaps not *wide*, intrusions into privacy. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (considering the validity of using thermal imaging on one's home); *United States v. Jones*, 565 U.S. 400, 402–03 (2012) (construing "the attachment of a [GPS] tracking device to an individual's vehicle" for twenty-eight days); *Carpenter*, 138 S. Ct. at 2217 n.3 (considering whether "accessing seven days of [an individual's cell site location information] constitutes a Fourth Amendment search").

At base, these matters are best left to legislatures. *See* Zach Whittaker, *A Bill to Ban Geofence and Keyword Search Warrants in New York Gains Traction*, TechCrunch (Jan. 13, 2022), https://tcrn.ch/35mLHkP (discussing a recently introduced New York bill that would ban the use of geofence warrants statewide). This case has arisen because no extant legislation prevents Google or its competitors from collecting and using this vast amount of data. And, as discussed below, despite its ongoing efforts to improve, Google appears to do so under the guise of consent few people understand how to disable. Even with consent, it seems clear that most Google users do not know how the consent flow to control their collection of data works, nor do they know Google is logging their location 240 times a day. It is not within this Court's purview to decide such issues, but it urges legislative action. Thoughtful legislation could not only protect the privacy of citizens, but also could relieve companies of the burden to police law enforcement requests for the data they lawfully have.

B. Because the Government Lacked Particularized Probable Cause as to Every Google User in the Geofence, the Warrant Violates the Fourth Amendment

At base, this particular Geofence Warrant is invalid. The Fourth Circuit has clearly articulated that warrants, like this one, that authorize the search of every person within a

particular area must establish probable cause to search every one of those persons. Here, however, the warrant lacked any semblance of such particularized probable cause to search each of its nineteen targets, and the magistrate thus lacked a substantial basis to conclude that the requisite probable cause existed. And to the extent the Government would argue that Steps 2 and 3 cure the warrant's defects as to probable cause, such an argument is unavailing here. The Government itself contends that law enforcement demonstrated probable cause to obtain *all* the data sought without any narrowing measures (*i.e.*, de-anonymized and geographically unlimited data from everyone within the geofence). In any event, Steps 2 and 3—undertaken with no judicial review whatsoever—improperly provided law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions. These steps therefore cannot buttress the rest of the warrant, as they fail independently under the Fourth Amendment's particularity prong.

1. Legal Standard: The Warrant Requirement

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Stated another way, the Fourth Amendment requires that a warrant (1) be supported by probable cause; (2) particularly describe the place to be searched and the things to be seized; and, (3) be issued by a neutral, disinterested magistrate.[31] *Dalia v. United States*, 441 U.S. 238, 255 (1979) (internal quotations and citations omitted). If a warrant is invalid, the proper remedy in a criminal action is "ordinarily" to suppress the evidence derived from it. *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018).

[31] Because this third prong intersects with the Court's good faith analysis, the Court discusses it more fully in Part III.C.2, *infra*.

a. Probable Cause

Whether probable cause for a search exists is a "practical, common-sense" question, asking whether "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). It requires only "the kind of fair probability on which reasonable and prudent people, not legal technicians," would rely. *United States v. Jones*, 952 F.3d 153, 158 (4th Cir. 2020) (citing *Florida v. Harris*, 568 U.S. 237, 244 (2013)). Officers must present sufficient information to the magistrate judge[32] to allow him or her to exercise independent judgment. *Gates*, 462 U.S. at 239. The magistrate cannot simply ratify the bare conclusions of others. *Id.* "When reviewing the probable cause supporting a warrant, a reviewing court must consider only the information presented to the magistrate who issued the warrant." *United States v. Wilhelm*, 80 F.3d 116, 118 (4th Cir. 1996) (citations omitted). "[T]he duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004).

More specifically, a warrant must be "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006) (quoting *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002)). Indeed, the United States Court of Appeals for the Fourth Circuit has established that warrants that authorize the search of "all persons on [a] premise[s]" must show probable cause "to believe that *all* persons on the premises at the time of the search are involved in the criminal activity." *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) (emphasis added) (second alteration in original), *overturned on other grounds by Pearson v. Callahan*, 129 S. Ct. 808 (2009). In other words, these warrants must demonstrate

[32] In the federal system, the magistrates who review and sign search warrants are judges who must have law degrees. This is not necessarily the case in state judicial systems.

"good reason to suspect or believe that anyone present at the anticipated scene will probably be a participant in the criminal activity." *Owens*, 372 F.3d at 276 (internal quotation marks omitted).

At base, probable cause demands that law enforcement possess "a reasonable ground for belief of guilt . . . *particularized* with respect to the person to be searched or seized." *Maryland v. Pringle*, 124 S. Ct. 795, 800 (2003) (emphasis added); *see Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) ("Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person.") A "person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra*, 444 U.S. at 91.

b. Particularity

A warrant must also be sufficiently "particular[]." *Hurwitz*, 459 F.3d at 470. Thus, a warrant must "confine the executing [officers'] discretion by allowing them to seize only evidence of a particular crime." *United States v. Cobb*, 970 F.3d 319, 328 (4th Cir. 2020), as amended (Aug. 17, 2020) (quoting *United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986)). The warrant must therefore "identif[y] the items to be seized by their relation to designated crimes," and the "description of the items [must] leave[] nothing to the discretion of the officer executing the warrant." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (citation omitted). "So long as the warrant describes the items to be seized with enough specificity that the executing officer is able to distinguish between those items which are to be seized and those that are not . . . the particularity standard is met." *United States v. Blakeney*, 949 F.3d 851, 862 (4th Cir. 2020) (internal citations and quotations omitted).[33]

[33] The Framers included the particularity requirement to "end the practice, abhorred by the colonists, of issuing general warrants," which authorized officers to carry out an "exploratory rummaging in a person's belongings." *United States v. Dargan*, 738 F.3d 643, 647 (4th Cir. 2013) (internal citation and quotations omitted). Such "general warrants" placed "the liberty of

2. The Geofence Warrant Fails to Establish Particularized Probable Cause to Search Every Google User Within the Geofence

Although cloaked by the complexities of novel technology, when stripped of those complexities, this *particular* Geofence Warrant lacks sufficient probable cause.[34] The United States Supreme Court has explained that warrants must establish probable cause that is "particularized with respect to the person to be searched or seized." *Pringle*, 124 S. Ct. at 800. This warrant did no such thing. It first sought location information for *all* Google account owners who entered the geofence over the span of an hour.[35] For those Google accounts, the warrant further sought "contextual data points with points of travel outside of the" Geofence for yet another hour—and those data points retained *no* geographical restriction. (ECF No. 54-1, at 4.) Astoundingly, the Government claims that law enforcement established probable cause to obtain *all* information (Steps 1, 2, and 3) from *all* users within the geofence without any

---

every [person] in the hands of every petty officer" and were therefore denounced as "the worst instrument of arbitrary power." *Stanford v. Texas*, 379 U.S. 476, 481 (1965).

[34] In considering whether the Geofence Warrant is valid, the Court assumes for the sake of analysis that the Government's collection of data here is a "search." *See In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 736 (noting that by obtaining a warrant and arguing for the validity of that warrant, "the [G]overnment is treating its proposed capture of information as a search"). Indeed, this is the position Google advances in its amicus brief.

[35] To be clear, the Court sees individuals from whose accounts the Government obtained data as functional subjects of the search, even though the warrant authorized officers to obtain data only from Google's servers. In the same way that users' devices generate IP address information and typically share that information with a third party, so too do users' phones generate Location History data and share that information with Google. *See, e.g.*, *United States v. Broy*, 209 F. Supp. 3d 1045, 1053 (C.D. Ill. 2016) (treating the defendant's IP address as if it is were defendant's property that he disclosed to a third party).

In other words, regardless of which entity's files the Government looked through, the users ultimately retain at least some joint interest in the location data their phones generate. As discussed in Part III.B.4, *infra*, however, because the Court ultimately finds that Det. Hylton acted in good faith, whether these individuals have an expectation of *privacy* in that data must be decided another day. *Cf., e.g.*, *Broy*, 209 F. Supp. 3d at 1053 (finding no reasonable expectation of privacy because the defendant disclosed his IP address to a third party).

narrowing measures.[36] Yet the warrant simply did not include any facts to establish probable cause to collect such broad and intrusive data from each one of these individuals.

Law enforcement attempted to justify the warrant by claiming that such a sweeping search "may [have] tend[ed] to identify potential witnesses and/or suspects." (ECF No. 54-1, at 7.) Even if this Court were to assume that a warrant would be justified on the grounds that a search would yield *witnesses* (some of whom had already been interviewed) instead of perpetrators, the Geofence Warrant is completely devoid of any suggestion that all—or even a substantial number of—the individuals searched had participated in or witnessed the crime. *Cf. Owens*, 372 F.3d at 276. To be sure, a fair probability may have existed that the Geofence Warrant would generate the *suspect's* location information.[37] However, the warrant, on its face, also swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny.

Indeed, it is difficult to overstate the breadth of this warrant, particularly in light of the narrowness of the Government's probable cause showing. Law enforcement knew only that the perpetrator "had a cell phone in his right hand and appeared to be speaking with someone on the device." (ECF No. 54-1, at 6.) After the police failed to located the suspect via reviewing camera footage, speaking with witnesses, and pursuing two leads, law enforcement simply drew

---

[36] Instead, it appears that law enforcement implemented narrowing measures in this Warrant at the behest of Google. (*See* ECF No. 202, at 275–76 (discussing "go bys," template documents that outline "specific information that [Google] need[s] in order to process the search warrant").)

[37] For instance, Det. Hylton stated in his affidavit that: (1) surveillance tapes revealed that the suspect used a phone; (2) in the officer's "training and experience, when people act in concert . . . they frequently utilize cellular telephones;" (3) Google "provides electronic communication services to subscribers, including email services;" (4) Google "has also developed a proprietary operating system for mobile devices, including cellular phones, known as Android;" and, (5) studies show that "91% of American adults own a cellular phone with 56% being smartphones." (ECF No. 54-1, at 6–7.)

a circle with a 150-meter radius that encompassed the Bank, the entirety of the Church, and the Church's parking lot.[38] The Government then requested location information for *every device* within that area. *See Carpenter*, 138 S. Ct. 2206, 2216 (2018) (describing cell phone location information as "encyclopedic").

What is more, in one instance, this Geofence Warrant captured location data for a user who may not have been *remotely* close enough to the Bank to participate in or witness the robbery. Because the radius of one of the users' confidence intervals stretched to around 387 meters, the Geofence Warrant might have reported that user's location data to the Government, notwithstanding the fact that he may have simply been present in any number of nearby locations. For example, that person may have been dining inside the Ruby Tuesday restaurant nearby. The person may have been staying at the Hampton Inn Hotel, just north of the Bank. Or, he or she could have been inside his or her own home in the Genito Glen apartment complex or the nearby senior living facility. He or she may have been moving furniture into the nearby self-storage business. Indeed, the person may have been simply driving along Hull Street or Price Club Boulevard. Yet the Government obtained the person's location data just the same. The Government claims that footage depicting the perpetrator holding a phone to his ear—and nothing else—justified this sweeping warrant. That, however, is simply not "[]reasonable." U.S. Const. amend. IV.

To further underscore the breadth of this search, Chatrie's expert Spencer McInvaille pointed out a likely "false positive" from the warrant—"Mr. Blue." McInvaille testified that this

---

[38] The Government has made passing references to "several [additional] pieces of evidence" that might have guided the contours of the Geofence Warrant. (*E.g.*, ECF No. 202, at 272.) But neither the warrant nor its supporting affidavit referred to this evidence. It is therefore irrelevant to the validity of the warrant. *See Groh v. Ramirez*, 540 U.S. 551, 557–58 (2004) (declining to consider material contained in a warrant's *application* where the warrant did not incorporate the application by reference).

"false positive" individual may not have ever stepped within the geofence—he may have simply driven "outside of the original geofence" on a nearby road, but could have nonetheless appeared "as if [he] were inside the geofence." (ECF No. 201, at 43–44, 65.) Because Google's location estimate for that person could have been "incorrect," Google may have *thought* the person had stepped foot in the target area. (ECF No. 201, at 43–44.) The Government therefore obtained two hours of unrestricted location data for an individual who perhaps had only driven within the outer vicinity of the crime scene.[39]

This Geofence Warrant therefore suffers from the same probable cause defect as that at issue in *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020). In that case, the Government sought "to erect three geofences." *Id.* 732. Two encompassed the same location during different timeframes, and the other captured a second location. *Id.* Each geofence lasted for forty-five minutes. *Id.* The court remarked that "the proposed warrant would admittedly capture the device IDs . . . for all who entered the geofences, which surround locations as to which there is no reason to believe that anyone – other than the Unknown Subject – entering those locations is involved in the subject offense or in any other crime." *Id.* at 752. There, just as here, the warrant provided the Government "unlimited

[39] The fact that data points obtained during Steps 1 and 2 are anonymized when Google reports them does not completely quell this Court's concerns about the invasiveness of this warrant. Even "anonymized" location data—from innocent people—can reveal astonishing glimpses into individuals' private lives when the Government collects data across even a one or two hour period. As noted above, during the March hearing, McInvaille identified three anonymous accounts captured within the geofence—"Mr. Blue," "Mr. Green," and "Ms. Yellow." (ECF No. 201, at 63–71.)

McInvaille testified that, using two hours of only "anonymized" data obtained through the warrant, he could observe each account's reported location, track each account to his or her home, and pinpoint each account's personal identity using publicly available resources even without any Step 3 information. *See* Herbert B. Dixon Jr., *Your Cell Phone is a Spy!*, Am. Bar Ass'n (July 29, 2020), https://bit.ly/3nRuCVq ("Although user data are anonymized, users' identities can nonetheless be determined by following their movements back to their homes and other places.").

discretion to obtain from Google the device IDs . . . of anyone whose Google-connected devices traversed the geofences (including their vaguely defined margins of error), based on nothing more than the 'propinquity' of these persons to the Unknown Subject at or near the time" of the criminal activity. *Id.* at 753. As that court (and the Supreme Court in *Ybarra*) recognized—and as this Court now concludes—the Fourth Amendment's probable cause requirement demands more than "mere propinquity" to a crime. *Id.* at 752; *Ybarra*, 444 U.S. at 91.

Despite the Government's reliance on *United States v. McLamb*, that case is inapposite. There, the Fourth Circuit upheld a warrant that allowed law enforcement to obtain identifying information of "any user entering a username and password into" an internet-based dark website where users could download or upload child pornography. *United States v. McLamb*, 880 F.3d 685, 689 (4th Cir. 2018). But there, a user's "mere propinquity" to the website *did* necessarily establish probable cause: any user visiting the site likely participated in the criminal conduct of viewing or sharing child pornography. *Id.* Here, on the other hand, a Google user's proximity to the bank robbery does not necessarily suggest that the user participated in the crime. *McLamb* therefore does not inform this case.[40]

Nor does the Government's reliance on *United States v. James* persuade. The *James* court considered a warrant to collect cell tower information (so-called "tower dumps") to determine whether "a particular cellular phone number (ostensibly held by the robber) could be identified during the timeframes of each of the respective robberies." 2018 WL 6566000, at *1.

[40] But one can readily imagine other instances when one's "mere propinquity" to a location, as in *McLamb*, likely *would* provide probable cause to obtain location data for each individual within a geofence. This would *not* necessarily involve improper use of location data. For example, the FBI appears to have employed geofence technology to locate participants in the January 6 Capitol riots. Mark Harris, *How a Secret Google Geofence Warrant Helped Catch the Capitol Riot Mob*, Wired (Sept. 30, 2021), https://bit.ly/3HktvWU. In that situation, one's presence within the Capitol *would* perhaps, by itself, provide probable cause that an individual was present without permission and was therefore committing a crime.

Law enforcement sought the cell tower data based on the notion that a cell phone number present at the location and time of all six robberies created sufficient probable cause that the number belonged to the robber. *Id.* Ultimately, the court concluded that "there was a fair probability that data from the cellular towers" would contain identifying information about the perpetrator and that therefore the warrants sufficed to allege probable cause. *Id.* at *4. As another court has noted however, *James* did not account for whether probable cause existed to search through the *other* individuals' location information. *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 751; *see also id.* at 752 (distinguishing another tower dump decision from the geofence context because the court discussing the tower dump "stopped the analysis once the court found probable cause in the 'nexus' between the offense and *all* the requested cell phone records, without analyzing whether probable cause existed to obtain all of those records." (quoting *In re Search of Cellular Telephone Towers*, 945 F. Supp. 2d 769 (S.D. Tex. 2013)). *James* therefore stopped short of considering whether "particularized" probable cause existed, and it is precisely that lack of narrowly-tailored probable cause that is fatal to this Geofence Warrant.[41]

The Court cautions that it declines to consider today whether a geofence warrant may *ever* satisfy the Fourth Amendment's strictures. *See In re Search Warrant Application for*

---

[41] Throughout this litigation, the parties—and Google—drew or resisted analogies to tower dumps. As explained above, however, the lead tower dump cases like *James* do not persuade this Court. Those decisions either decide that individuals' proximity to certain towers *alone* creates probable cause to search them, or altogether neglect to consider such particularity concerns. *James*, 2018 WL 6566000, at *4; *see also United States v. James*, 3 F.4th 1102, 1106 (8th Cir. 2021) (affirming the district court's adoption of the magistrate judge's original opinion on the same grounds). Indeed, the Eighth Circuit in *James* expressly warned that in holding valid the warrants at issue—which connected a robber to a *series* of crimes—was *not* holding "that it is now fair game to search the records from 'cell phone towers near the location of *every* crime.'" *Id.* at 1106. The Court similarly concludes here that the commission of a single crime—by itself, and with no narrowing measures or guardrails—is not sufficient to search geofence records "near the location of *every* crime." *Id.*

Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 361–62 (N.D. Ill. 2020) ("[I]t is nearly impossible to pinpoint a search where only the perpetrator's privacy interests are implicated."). Consider, for example, one of the few other federal court opinions to address a geofence warrant—*In re Search of Information That Is Stored at the Premises Controlled by Google LLC*, No. 21sc3217, 2021 WL 6196136 (D.D.C. Dec. 30, 2021) [hereinafter "DDC Opinion"]. There, law enforcement devised a two-step process to narrow the list of individuals whose data they would obtain. *Id.* at *5–6. At Step 1, Google would identify all accounts who entered the geofence within the relevant time periods. *Id.* For each of these accounts, Google would turn over only anonymized data. *Id.*

The Government would then review that data, identify likely suspects based on the "mov[ement]" of the users' devices through the geofence, and, crucially, identify to the *court* the devices the Government believed belonged to the perpetrator. *Id.* The *court* could then, at its discretion, order Google to disclose to the Government personally identifying information for devices that belonged to likely suspects. *Id.* In essence, to obtain a warrant authorizing disclosure of de-anonymized data, the Government was required to demonstrate that location data for a *particular* user or set of users would provide evidence of the crime. And crucially, the warrant left ultimate discretion as to which users' information to disclose to the reviewing court, not to Google or law enforcement.

In certain situations, then, law enforcement likely *could* develop initial probable cause to acquire from Google *only* anonymous data from devices within a narrowly circumscribed geofence at Step 1. *See Hurwitz*, 459 F.3d at 473 (a warrant must be "no broader than the probable cause on which it is based"). From there, officers likely could use that narrow, anonymous information to develop probable cause particularized to specific users. Importantly,

officers likely could then present that particularized information to a magistrate or magistrate judge to acquire successively broader and more invasive information. Although the *instant* warrant is invalid, where law enforcement establishes such narrow, particularized probable cause through a series of steps with a court's authorization in between, a geofence warrant may be constitutional.[42]

At bottom however, particularized probable cause "cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be." *Ybarra*, 444 U.S. at 91. The Court finds unpersuasive the United States' inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby. In essence, the Government's argument rests on precisely the same "mere propinquity to others" rationale the Supreme Court has already rejected as an appropriate basis for a warrant. *Id.* This warrant therefore cannot stand.

---

[42] The warrant in the DDC Opinion differed in additional ways. For instance, that warrant appears to have sought only location data that fell *within* the geofence across time periods notably shorter than the geofence at bar. *See* DDC Op. at *12 ("[T]he geofence only provides cell phone user's whereabouts in a single area for a handful of minutes on the days in question, not the sum-total of their daily movements."). Here, by contrast, the Government sought two hours of location data *not* bound within the geofence. *Cf.* DDC Op. *12 ("[T]he warrant does not seek location data for days or even hours to track the whereabouts of the perpetrators, but rather location data that is tailored and specific to the time of the [alleged crimes] only." (second alteration in original) (quotation marks and citation omitted)).

In addition to restricting officers' discretion when selecting which accounts for which to obtain personally identifying information, limiting the pool of data returned to only location points *within* the geofence helps assuage this Court's concerns with respect to particularized probable cause, and, more broadly, concerns that broad swaths of anonymous data can be used to pinpoint numerous individuals' identities.

3. This Geofence Warrant's Three-Step Process Does Not Cure Its Defects

To the extent the Government would attempt to argue in the alternative that this warrant's three-step process cures any defects with the warrant's particularized probable cause, such an argument is unavailing.[43] Even if this narrowing process cured any of the warrant's shortcomings as to particularized probable cause, this process cannot independently buttress the warrant for an entirely separate reason: clear lack of particularity. Warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. In other words, "[a] warrant that meets the particularity requirement leaves the executing officer with no discretion as what to seize." *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (citing *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). But Steps 2 and 3 of this warrant leave the executing officer with *unbridled* discretion and lack any semblance of objective criteria to guide how officers would narrow the lists of users.

This warrant, for instance, contains no language objectively identifying *which* accounts for which officers would obtain further identifying information. Nor does the warrant provide objective guardrails by which officers could *determine* which accounts would be subject to further scrutiny. Nor does the warrant even simply limit the *number* of devices for which agents could obtain identifying information. Instead, the warrant provided law enforcement unchecked discretion to seize more intrusive and personal data with each round of requests—without ever needing to return to a neutral and detached magistrate for approval.

[43] The Court recognizes that the Government primarily argues that it possessed probable cause to obtain *all* data sought regardless of the three-step process.

The facts here underscore the breadth of discretion law enforcement possessed under this warrant.[44] After receiving anonymized information on the nineteen targeted users at Step 1, Det. Hylton requested the additional location information (Step 2) and subscriber information (Step 3) "for all 19 device numbers produced in [S]tep 1." (ECF No. 96-2, at ¶ 15.) In response, a Google specialist "called Detective Hylton and explained the issues in the Detective's email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant."[45] (ECF No. 96-2, at ¶ 16.) During that call, "[t]he LIS specialist also explained the importance of [S]tep 2 in narrowing." (ECF No. 96-2, at ¶ 16.) Det. Hylton eventually narrowed his requests. Yet he did not specify to Google why he was choosing these particular users.

Google's insistence on narrowing the list does not render this warrant sufficiently particular. For one thing, this warrant's clear text does not specifically allow Google to limit the group of accounts that would be subject to further scrutiny. (*See* ECF No. 54-1, at 4–5 (noting only that Google "shall produce" further information).) But even if it did, Fourth Amendment discretion must be confined to the signing magistrate, not the executing officers or a third party. *United States v. Chadwick*, 433 U.S. 1, 9 (1977) ("The judicial warrant has a significant role to play in that it provides the detached scrutiny of a neutral magistrate . . . ."), *abrogated on other*

[44] The facts also raise a concern about how even good faith effort by law enforcement can impinge upon constitutional boundaries through a lack of understanding as to what this warrant actually produces and how it does so. While all performed in good faith—especially given this novel and complex process—Det. Hylton returned the warrant before it was served, improperly requested Step 2 and 3 information simultaneously, failed at first to narrow his request at Step 2, and incorrectly tried to add a Step 4 to the process. While the Google LIS allowed only what was permitted under the warrant (which Det. Hylton did not resist), Fourth Amendment protections should not be left in the hands of a private actor.

[45] Det. Hylton received this remonstration despite having executed three geofence warrants prior to this one.

grounds by California v. Acevedo, 500 U.S. 565 (1991). Stated plainly, Steps 2 and 3 "put[] no limit on the [G]overnment's discretion to select the device IDs from which it may then derive identifying subscriber information from among the anonymized list of Google-connected devices that traversed the geofences." *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 754. These Steps accordingly fail to provide the executing officer with clear standards from which he or she could "reasonably . . . ascertain and identify . . . the place to be searched [or] the items to be seized." *Blakeney*, 949 F.3d at 861. The Government therefore cannot rely on Steps 2 and 3 to supply this warrant with particularized probable cause, as these steps independently fail under the Fourth Amendment's particularity requirement.

4. The Third-Party Doctrine

Lastly, the Court simply cannot determine whether Chatrie "voluntarily" agreed to disclose his Location History data based on this murky, indeterminate record. But the Court expresses its skepticism about the application of the third-party doctrine to geofence technology. Under this doctrine, "a person [generally] has no legitimate expectation of privacy in information he [or she] voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). However, in *Carpenter v. United States*, the Supreme Court refined this principle and held than an individual *does* possess an expectation of privacy in seven days of cell-site location information collected by a wireless carrier. 138 S. Ct. at 2217 & n.3. Here, the Government argues that Chatrie cannot claim a reasonable expectation of privacy in his Location History data because (1) he "voluntarily disclosed" the information to Google; and, (2) the two hours of location data sought here do not implicate the same privacy concerns as the seven days obtained in *Carpenter*. (ECF No. 41, at 11; *see* ECF No. 41, at 9–13.)

The Court thinks otherwise. Common sense underscores Supreme Court Justice Sonia Sotomayor's observation in *United States v. Jones* about "voluntary" collection of electronic information unbeknownst to the subject of the warrant. As to the third-party doctrine, Justice Sotomayor observed that:

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties [because] [t]his approach is ill suited to the digital age. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year.

Jones, 565 U.S. at 417–18 (Sotomayor, J., concurring). At base, the topic is complex. And considering the messiness of the current record as to how and when Chatrie "gave consent," the Court cannot—and need not—reach a firm decision on the issue. But the Court remains unconvinced that the third-party doctrine would render hollow Chatrie's expectation of privacy in his data, even for "just" two hours. Google Location History information—perhaps even more so than the cell-site location information at issue in *Carpenter*—is "detailed, encyclopedic, and effortlessly compiled." *Carpenter*, 138 S. Ct. at 2216; *see id.* at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."). Although, unlike in *Carpenter*, Chatrie apparently took some affirmative steps to enable location history, those steps likely do not constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day.

This is especially so given the limited and partially hidden warnings provided by Google. In the Google Assistant set-up process, the device likely provided Chatrie a single pop-up screen informing him that "[t]his data may be saved and used in any Google service where [he was] signed in to give [him] more personalized experiences," and that he "can see [his] data, delete it

and change [his] settings at account.google.com." (ECF No. 147, at ¶ 7; *see* ECF No. 96-1, at ¶ 7; ECF No. 201, at 102; ECF No. 202, at 21.) However, the consent flow did not detail, for example, how frequently Google would record Chatrie's location (every two to six minutes); the amount of data Location History collects (essentially *all* location information); that even if he "stopped" location tracking it was only "paused," meaning Google retained in its Sensorvault all his past movements; or, how precise Location History can be (*i.e.*, down to twenty or so meters).[46] (ECF No. 201, at 122, 136; ECF No. 202, at 71.)

While the Court recognizes that Google puts forth a consistent effort to ensure its users are informed about its use of their data, a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting "YES, I'M IN" at midnight while setting up Google Assistant, even if some text offered warning along the way. The record here makes plain that these "descriptive texts" are less than pellucid. Although the Court cannot reach a final decision on the issue today based on the current record here, Chatrie likely could not have, in a "meaningful sense, . . . voluntarily 'assumed the risk' of turning over a comprehensive dossier of his physical movements" to law enforcement. *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745); *see id.* at 2217 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

[46] As Google's expert Marlo McGriff testified, Location History also allows Google to estimate a device's *elevation*. Thus, if New York City law enforcement obtained a geofence warrant with a roughly 150-meter radius (similar in size to the one at issue here) that encircled the Empire State Building, even if it were not fully precise, the police might be able to obtain location data for many thousands of people.

C. Because Det. Hylton Consulted with Government Attorneys in the Face of Novel Technology and Obtained Similar Warrants in the Past, and Because the Warrant Was Not Otherwise "So Facially Deficient," the Good-Faith Exception Applies

Despite the warrant's defects, the Court ultimately cannot find that excluding the instant evidence would serve to deter future improper law enforcement conduct. This is particularly so in light of rapidly advancing technology and lack of judicial guidance on this novel investigatory technique, and where, as here, prosecutors and magistrates approved three similar warrants.

1. Legal Standard

The exclusionary rule "is neither 'a personal constitutional right' nor is it 'designed to redress the injury occasioned by an unconstitutional search.'" *United States v. Manafort*, 323 F. Supp. 3d 795, 805 (E.D. Va. 2018) (quoting *Davis v. United States*, 564 U.S. 229, 236 (2011)). Rather, the exclusionary rule "is a prudential doctrine created . . . to compel respect for" constitutional rights. *Davis*, 564 U.S. at 236–37 (2011). "[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *McLamb*, 880 F.3d at 690 (internal quotation marks and citation omitted). Where suppression would not produce deterrent benefits, the exclusionary rule does not apply. *United States v. Leon*, 468 U.S. 897, 909 (1984).

For that reason, evidence obtained pursuant to a search warrant issued by a neutral magistrate need not be excluded if the officer's reliance on the warrant was "objectively reasonable." *Id.* at 922–23. Generally, the fact that a neutral magistrate has issued a warrant "suffices to establish" that a law enforcement officer has "acted in good faith in conducting the search." *Id.* at 922. Therefore, searches carried out pursuant to a warrant "rarely require any deep inquiry into reasonableness." *Id.*

The Fourth Circuit has nonetheless set out four categories of cases in which the good-faith exception will not apply:

> (1) if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) if the issuing magistrate wholly abandoned his [or her] judicial role[;] . . . (3) if the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) if under the circumstances of the case the warrant is so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized-that the executing officers cannot reasonably presume it to be valid.

United States v. Doyle, 650 F.3d 460, 467 (4th Cir. 2011) (internal quotation marks and citations omitted). When considering a motion to suppress the fruits of a novel investigative technique, courts generally decline to hold a warrant "facially deficient where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant." *McLamb*, 880 F.3d at 691. Further, "consultation [with Government attorneys prior to seeking a warrant] is a relevant consideration in determining whether the warrant was facially deficient." *United States v. Matthews*, 12 F.4th 647, 657 (7th Cir. 2021).

2. Because Det. Hylton Relied on the Approval of Prior Warrants in the Face of Novel Technology, the Good-Faith Exception Applies

a. Det. Hylton

Despite the warrant failing under Fourth Amendment scrutiny, the *Leon* good faith exception shields the resulting evidence from suppression. The warrant lacked particularized probable cause, but it was not "*so* lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Leon*, 468 U.S. at 923 (emphasis added). This is particularly so because "the legality of [this] investigative technique [was] unclear," and Det. Hylton sought "advice from counsel before applying for the warrant." *McLamb*, 880 F.3d at 691. When Det. Hylton applied for the Geofence Warrant, no court had yet ruled on the

legality of such a technique. And as this Court's preceding analysis demonstrates, the permissibility of geofence warrants is a complex topic, requiring a detailed, nuanced understanding and application of Fourth Amendment principles, which police officers are not and cannot be expected to possess. *See* Part III.B.2, *supra*.[47]

In the face of this legal uncertainty, Det. Hylton relied on his past experience seeking geofence warrants—he had sought three before applying for this one. Magistrates and prosecutors had approved all three. *See Matthews*, 12 F.4th at 656 (noting the "general principle that attorney involvement supports a finding of good faith"). Det. Hylton testified that these prior warrants were "mostly similar" to the one at bar—all but one incorporated a roughly 150-meter radius, although a "few of them had more locations because of the more robberies to investigate." (ECF No. 202, at 328.) Even accounting for his miscues, in light of the complexities of this case, Det. Hylton's prior acquisition of three similar warrants, and his consultation with Government attorneys before obtaining those warrants, the Court cannot say that Det. Hylton's reliance on the instant warrant was objectively unreasonable. *See McLamb*, 880 F.3d at 691. While magistrate approval and consultation with the prosecution alone cannot and should not mechanically trigger the good-faith exception, exclusion here likely would not "meaningfully deter" improper law enforcement conduct. *Herring v. United States*, 555 U.S. 135, 144 (2009).[48]

---

[47] The Court therefore rejects Chatrie's argument that "one who had even a rudimentary understanding of the Fourth Amendment's particularity and breadth requirements" would know that this warrant was insufficient. (ECF No. 205, at 42.)

[48] This is particularly so because Det. Hylton's "consultation with [G]overnment attorneys [in the face of untested investigatory techniques] is precisely what *Leon*'s 'good faith' expects of law enforcement." *McLamb*, 880 F.3d at 691.

b. Magistrate Bishop

Nor can this Court conclude that Magistrate Bishop wholly abandoned his role as a detached magistrate as Chatrie argues. *See Doyle*, 650 F.3d at 470. This exception to good faith primarily looks to whether the magistrate "overstep[ped] his [or her] judicial responsibilities and compromise[d] his judicial neutrality," *United States v. Gary*, 420 F. Supp. 2d 470, 486 (E.D. Va. 2006) (quoting *United States v. Servance*, 394 F.3d 222, 231 (4th Cir. 2005), *vacated on other grounds by Servance v. United States*, 544 U.S. 1047 (2005)), by, for example, actively participating in an investigation, *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 327 (1979); retaining a pecuniary interest in issuing the warrant, *Connally v. Georgia*, 429 U.S. 245, 249–51 (1977) (per curiam); "rubber stamp[ing]" a warrant that contained a "bare bones" affidavit, *Wilhelm*, 80 F.3d at 121 (4th Cir. 1996); or, failing to make an independent assessment as to the validity of the warrant, *United States v. McKneely*, 810 F. Supp. 1537, 1547 (D. Utah 1993), *rev'd on other grounds by United States v. McKneely*, 6 F.3d 1447 (10th Cir. 1993).

Chatrie has, perhaps, shown that Magistrate Bishop *should have* considered the implications of the Warrant more carefully. But ultimately, he has "produced no evidence to show that the magistrate did not read the affidavit or that he read it so cursorily as to have wholly abandoned his neutral and detached role." *Gary*, 420 F. Supp. 2d at 487; (*see* ECF No. 202, at 361–62 (noting that the magistrate reviewed the warrant for around fifteen or thirty minutes).) Nor did he "suggest that the magistrate acted in a partisan manner or aligned himself with the police. Consequently, . . . the second [*Leon* exception] does not bar application of the good-faith exception." *Gary*, 420 F. Supp. 2d at 487. Chatrie further argues that "[t]he magistrate's utter lack of concern regarding the obvious flaws in the warrant constituted a complete abandonment of his role as . . . neutral arbiter." (ECF No. 205, at 41.) But the Fourth Circuit has instructed

that such "an allegation that a search warrant application contained grossly insufficient information is best analyzed under the third *Leon* exception." *United States v. Wellman*, 663 F.3d 224, 229 (4th Cir. 2011). And for the reasons explained above, that exception does not warrant suppression either.

Finally, the Court must address Chatrie's challenge to Magistrate Bishop's qualifications. Chatrie contends that Magistrate Bishop did not possess the requisite statutory qualifications to make the instant probable cause determination. The Court first observes that, in Virginia, any United States citizen who is a resident of the Commonwealth is eligible to be appointed as a magistrate with certain limitations not relevant here. Va. Code § 19.2-37. To qualify today, a magistrate need only have "a bachelor's degree from an accredited institution of higher education." Va. Code § 19.2-37(B). And "[a] person initially appointed as a magistrate prior to July 1, 2008, who continues in office without a break in service is *not* required to have a bachelor's degree from an accredited institution of higher education." Va. Code § 19.2-37(B) (emphasis added). No law degree is required. Indeed, "[n]o person appointed as a magistrate on or after July 1, 2008, *may* engage in the practice of law." Va. Code § 19.2-37(F) (emphasis added).

Magistrate Bishop graduated from Pensacola Christian College with a Bachelor of Science Degree in Criminal Justice in May of 2016. He was appointed as a Virginia magistrate roughly two years later in June 2018, began certification school in July 2018, and was formally appointed and "released for independent service on October 24, 2018." (ECF No. 156, at ¶ 3.) His nine-month probationary period pursuant to Virginia Code § 19.2-38 ended on March 12, 2019. In other words, Magistrate Bishop had been serving as a non-probationary magistrate just

three months before he signed this sweeping and powerfully intrusive Geofence Warrant on June 14. And he had graduated from college just three years earlier.

Chatrie does not rest on Magistrate Bishop's lack of a law degree. He instead avers that Magistrate Bishop's undergraduate degree was not sufficiently "accredited" under Virginia law. (ECF No. 135, at 6–9.) As noted, Pensacola Christian College does not appear to be officially licensed in Florida. (*See* Ex. B 24, ECF No. 135-2 ("Pensacola Christian College operates in the state of Florida as an independent institution of higher learning that is exempt from state commission oversight as per Florida statutes.").) Further, it does not appear to be accredited by a regional higher-education accrediting agency. *See, e.g.*, Southern Association of Colleges and Schools Commission on Colleges, *Accredited and Candidate List January 2022* (last visited Mar. 1, 2022), https://bit.ly/3cb3ICF. Yet the Transnational Association of Christian Colleges and Schools ("TRACS")[49] accredited the college in 2013. *Pensacola Christian College*, TRACS (last visited Mar. 1, 2022), https://bit.ly/3C22S5j.

Chatrie contends that the TRACS accreditation means little, as "[t]he most widely respected agencies are regional [accrediting] bodies," while "national accrediting agencies are significantly less prestigious." (ECF No. 135, at 7.) He points out that elsewhere, the Virginia Code and Virginia Administrative Code specify that certain professionals receive degrees accredited by specific agencies (typically distinguishing between regional and national entities), and that professionals with similar levels of expertise are typically required to obtain a degree from a regionally accredited school. *See* Va. Code § 54.1-4400; 18 Va. Admin. Code 115-40-22, 160-40-280. If the Court is to read anything into this, however, it is precisely the opposite

[49] TRACS is a national agency recognized by the Council for Higher Education Accreditation and the United States Department of Education. *CHEA- and USDE- Recognized Accrediting Organizations*, CHEA (last visited Mar. 1, 2022), https://bit.ly/3og0sLw.

conclusion from Chatrie's. The notion that Virginia lawmakers narrow the permissive group of accrediting agencies *elsewhere* merely signals that the lawmakers know how to limit the pool of accrediting bodies but chose not to do so here. *Cf. Alexis v. Barr*, 960 F.3d 722, 735 n.1 (5th Cir. 2020) (Dennis, J., dissenting) (noting that where a statute defined a term more specifically in one place but not the other, lawmakers had "intentionally omitted" that more specific definition in the other usage). Under Virginia Code § 19.2-37 then, Magistrate Bishop's degree likely suffices.

To the extent Chatrie also attacks Magistrate Bishop's decision because he "would have had, at most, only a few months of experience evaluating warrant applications on his own when he signed the geofence warrant," that argument cannot prevail given Virginia's statutory scheme. (ECF No. 135, at 9.) Virginia magistrates must complete a training program, pass a certification examination, and serve a nine-month probationary period before hearing cases without supervision. Va. Code § 19.2-38. Magistrate Bishop had done this, and he had been certified by the Commonwealth of Virginia's Office of Executive Secretary. As a general principle, "[s]tates are entitled to some flexibility and leeway in their designation of magistrates, so long as all are neutral and detached and capable of the probable-cause determination required of them." *Shadwick v. City of Tampa*, 407 U.S. 345, 354 (1972). In the ordinary course then, Virginia sufficiently trains its magistrates to determine probable cause.

Frankly, however, it is not clear to the Court that *any* person just three years out of college should be burdened with the responsibility of approving or rejecting a warrant of this complexity and magnitude. The Court certainly does not impute any bad faith or improper action by Magistrate Bishop (or the Commonwealth). This case has shown, however, the myriad ways that geofencing instigates a massive intrusion into individual rights, and it does so without

notice to potentially thousands of persons with phones within it. It seems less than evident that all law enforcement officers have a clear understanding of the invasive scope of these warrants either. Nor do most magistrates, with or without a law degree. Ultimately, it is for the General Assembly to review or change its magistrate practice given this new technology, and one hopes they would.

In any event, even if Magistrate Bishop's degree or lack of experience did not qualify him to make this consequential finding, the good faith exception would still apply. The Fourth Circuit recently concluded in *McLamb* that the good faith exception is not categorically inapplicable even if the instant "warrant . . . reache[s] beyond the boundaries of a magistrate judge's jurisdiction" where suppression would not "produce an appreciable deterrence on law enforcement." 880 F.3d at 691 (internal quotation marks omitted). The Court finds that suppression based on a technical defect of the magistrate's credentials would not serve to deter improper law enforcement conduct. In a typical investigation, officers simply cannot be required to consult a magistrate's resume before approaching that magistrate to obtain a warrant.

IV. Conclusion

Despite the Court finding good faith here, the Court nonetheless strongly cautions that this exception may not carry the day in the future. This Court will not simply rubber stamp geofence warrants. If the Government is to continue to employ these warrants, it must take care to establish particularized probable cause. As the legal landscape confronts newly developed technology and further illuminates Fourth Amendment rights in the face of geofence practices, future geofence warrants may require additional efforts to seek court approval in between Steps, or to limit the geographic and temporal information sought. But in light of the complex legal issues that lead to this Court's conclusion, the Court cannot say that Det. Hylton's reliance on the

Geofence Warrant was objectively unreasonable. Accordingly, the *Leon* good faith exception applies, and the Court will deny Chatrie's motion to suppress evidence obtained as a result of the Geofence Warrant.

For the foregoing reasons, the Court will deny the Motion to Suppress. (ECF No. 29.)

An appropriate Order shall issue.

Date: 3-3-2022
Richmond, Virginia

/s/
M. Hannah Lauck
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA

v. **Criminal Case No. 3:19cr130**

OKELLO T. CHATRIE,

Defendant.

ORDER

For the reasons stated in the accompanying Memorandum Opinion, the Court DENIES Chatrie's Motion to Suppress. (ECF No. 29.)

It is SO ORDERED.

Date: 3-3-2022
Richmond, Virginia

/s/
M. Hannah Lauck
United States District Judge

FILED
MAY - 6 2022
CLERK, U.S. DISTRICT COURT
RICHMOND, VA

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	No. 3:19-CR-130
v.	Count 1: 18 U.S.C. §§ 2113(a), (d), (Credit Union Robbery)
OKELLO T. CHATRIE,	
Defendant.	Count 2: 18 U.S.C. § 924(c)(1)(A) (Use, Carry, and Brandish a Firearm During and in Relation to a Crime of Violence)
	Forfeiture Allegation

CRIMINAL INFORMATION

COUNT ONE
(Armed Credit Union Robbery)

On or about May 20, 2019, in the Eastern District of Virginia, the defendant, OKELLO T. CHATRIE, by force, violence, and intimidation, did take from the person and presence of another, namely J.W. and K.C., employees of the Call Federal Credit Union located at 3640 Call Federal Drive, Midlothian, Virginia, 23112, approximately $195,000 in United States currency, belonging to, and in the care, custody, control, management and possession of the Call Federal Credit Union, the accounts of which were then insured by the National Credit Union Administration Board, and in committing such offense, the defendant, OKELLO T. CHATRIE, did put in jeopardy the life of another person by the use of a dangerous weapon, that is a firearm.

(In violation of Title 18, United States Code, Sections 2113(a) and 2113(d)).

COUNT TWO
(Use, Carry, and Brandish a Firearm During and in Relation to a Crime of Violence)

On or about May 20, 2019, in the Eastern District of Virginia, the defendant, OKELLO T. CHATRIE, did knowingly and unlawfully use, carry, and brandish a firearm during and in

relation to a crime of violence for which he may be prosecuted in a court of the United States, that is, armed credit union robbery, as charged in Count One of this Information, which is re-alleged as if fully set forth here.

(In violation of Title 18, United States Code, Sections 924(c)(1)(A)(i) and (ii)).

FORFEITURE ALLEGATION

Pursuant to Federal Rule of Criminal Procedure 32.2, the defendant, OKELLO T. CHATRIE, is notified that if convicted of Count One of this Indictment, the defendant shall forfeit to the United States, any property, real or personal, which constitutes or is derived from proceeds traceable to such violation.

This property includes, but is not limited to:

A sum of money of at least $196,932.01, which represents the total proceeds of the offense charged, to be partially offset by $102,293 seized from 1317 Willis Street, Richmond, Virginia 23224 on August 13, 2019.

If the property subject to forfeiture cannot be located, the United States will seek an order forfeiting substitute assets.

The defendant is further notified that upon conviction of the offenses alleged in Count One or Count Two of this Indictment, the defendant shall forfeit any firearms and ammunition involved in or used in any knowing violation of such offenses.

Property subject to forfeiture includes, but is not limited to:

A 9 mm Taurus G2C pistol, serial number TLW87541; and

all accompanying ammunition.

(In accordance with Title 18, United States Code, Sections 924(d) and 981(a)(1)(C) as incorporated by Title 28, United States Code, Section 2461(c)).

JESSICA D. ABER
United States Attorney

By: 

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA

v.

OKELLO T. CHATRIE

Criminal No. 3:19CR130

May 9, 2022

COMPLETE TRANSCRIPT OF GUILTY PLEA
BEFORE THE HONORABLE M. HANNAH LAUCK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

Kenneth R. Simon, Jr., Assistant U.S. Attorney
Office of the U.S. Attorney
SunTrust Building
919 East Main Street, Suite 1900
Richmond, Virginia 23219

Counsel for the United States

Laura J. Koenig, Assistant Federal Public Defender
Office of the Federal Public Defender
701 E. Broad Street, Suite 3600
Richmond, Virginia 23219

Counsel for the Defendant

DIANE J. DAFFRON, RPR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT

(The proceedings in this matter commenced at 2:36 p.m.)

THE CLERK: Case No. 3:19CR130, *United States of America versus Okello T. Chatrie*.

Mr. Kenneth R. Simon, Jr. and Mr. Peter S. Duffey represent the United States. Ms. Laura J. Koenig represents the defendant.

Are counsel ready to proceed?

MR. SIMON: The United States is ready, Your Honor.

MS. KOENIG: Defense is ready, Your Honor.

Good afternoon.

THE COURT: Can you announce the case, please.

MR. SIMON: Good afternoon, Judge.

THE COURT: Good afternoon.

MR. SIMON: We are here for the plea agreement and plea hearing of the defendant in relation to a two-count criminal information charging the defendant in Count One with armed credit union robbery in violation of Title 18, United States Code, Sections 2113(a) and (d). And in Count Two, he's charged with carrying and brandishing a firearm during and in relation to that crime of violence in Count One.

There is a waiver of indictment in this case, a signed plea agreement, a statement of facts, as well as a consent order of forfeiture.

THE COURT: Can you please just put the maximum possible penalties on the record?

MR. SIMON: Yes, Judge. And with respect to Count One, the maximum penalty for that offense is 25 years' imprisonment, a $250,000 fine, a $100 special assessment, and a supervised release term of three years' imprisonment.

For Count Two, a mandatory minimum of seven years' imprisonment, a maximum term of life, a $250,000 fine, a supervised release term of five years, and a $100 special assessment.

THE COURT: All right. Are you prepared to proceed?

MS. KOENIG: We are, Your Honor.

THE COURT: All right. Why don't you both approach.

All right. Mr. Chatrie, I'm going to ask you a series of questions to make sure you understand the nature and the consequences of this plea. I'm going to ask you these questions under oath. If you were to be untruthful in response to anything I ask, you could be subject to different or additional penalties,

including perjury. Do you understand?

THE DEFENDANT: Yes, ma'am.

THE COURT: All right. So we're going to place you under oath.

(Sworn by the Clerk.)

THE COURT: All right. So, Mr. Chatrie, the first thing I want to go over with you is the fact that you have a right to go forward by way of indictment, not the criminal information that's in front of the Court. That would require a separate finding of probable cause by a grand jury.

I understand you know that right, and you're waiving it, and have signed a document to that effect today. Is that true?

THE DEFENDANT: Yes, ma'am.

THE COURT: And did you have plenty of time to speak to your counsel with respect to that issue?

THE WITNESS: Yes, ma'am.

THE COURT: And, Ms. Koenig, you had sufficient time to advise as to that?

MS. KOENIG: I did, Your Honor.

THE COURT: All right. Now, sir, I want to be sure you understand that at any time during this plea hearing, you can speak with your attorney. If you don't understand the question that I'm asking,

interrupt me and speak to her before you give me any kind of answer.

I also want you to know that you may choose to withdraw your guilty pleas at any time before I accept them today. Once I accept your guilty plea you cannot withdraw them except for what's called a just and fair reason. And that's a very high and difficult standard to meet under the law. Do you understand that?

THE DEFENDANT: Yes, ma'am.

THE COURT: All right. Now, I need to start by asking, are you the person named in the information? Are you correctly named? Are you Okello T. Chatrie?

THE DEFENDANT: Yes, Your Honor.

THE COURT: Have you drunk any alcohol or taken any drugs, prescription or otherwise, in the past 24 hours?

THE DEFENDANT: No, ma'am.

THE COURT: Have you ever been treated for any mental or emotional disorder or addiction of any kind?

THE DEFENDANT: No, ma'am.

MS. KOENIG: Your Honor, Mr. Chatrie is going through counseling right now for PTSD, and there may

be a diagnosis of complex trauma. I can't remember off the top of my head right now, but he is undergoing counseling for that. But that does not, in my experience with Mr. Chatrie, impact his competency or his ability to understand the plea or being able to proceed today.

THE COURT: All right. So, Mr. Chatrie, one thing I'm going to ask is for you please to speak into the microphone. It's the only way my court reporter can hear you.

But I understand you are receiving some counseling; is that true?

THE DEFENDANT: Yes, ma'am.

THE COURT: Is there anything about the counseling or your need for counseling that would affect your ability to understand what we're doing today?

THE DEFENDANT: No, ma'am.

THE COURT: Is there anything that would make you not be able to make a clear choice today?

THE DEFENDANT: No, ma'am.

THE COURT: I don't see that as I look at you, and your lawyer has just said so, but I need to follow-up.

All right, sir. This is so thorough, I have

to ask you. I know you can speak English because we're doing it, but can you read and write the English language? These are all written documents.

THE DEFENDANT: Yes, ma'am.

THE COURT: All right. How old are you, sir?

THE DEFENDANT: Twenty-seven, Your Honor.

THE COURT: Pardon me?

THE DEFENDANT: I'm 27, Your Honor.

THE COURT: Okay. And how far have you gone in school?

THE DEFENDANT: Grade 11.

THE COURT: All right. I want to confirm that you know the charges and the maximum possible penalties. The AUSA announced them in the criminal information and the maximum possible penalties.

First, let me ask you, Ms. Koenig are, you in agreement with what he put on the record?

MS. KOENIG: Yes, Your Honor, maximum sentence of 25 years on the armed robbery charge, and a minimum sentence of seven years to a maximum of life on the 924(c).

THE COURT: All right. The 924(c), does it have to be consecutive?

MS. KOENIG: It does, Your Honor.

THE COURT: All right. So, Mr. Chatrie, do

you understand what the AUSA said and what the maximum possible penalties are?

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. And you understand that Count Two would have to be consecutive to anything imposed as to Count One?

THE DEFENDANT: Yes, Your Honor.

THE COURT: Okay. Now, I want to be sure that you understand that these are felony pleas, and that by pleading guilty to them you're giving up valuable civil rights, and those include the right to vote, or hold public office, or possess any kind of firearm. Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: And if there are any immigration issues, it could involve removal or deportation and affect your ability to come back into the United States on a legal basis. Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. Now, have you had a sufficient opportunity to discuss the charges and the sentencing possibilities with your attorney before you came into this the courtroom today?

THE DEFENDANT: Yes, Your Honor.

THE COURT: Did you ask Ms. Koenig everything

about your case, including about the decision of whether or not to plead guilty and any defenses that you might have?

THE DEFENDANT: I think I did, Your Honor.

THE COURT: You think you did?

THE DEFENDANT: Yeah.

THE COURT: Well, I'm going to -- this is a big day, so if you have any other questions, this is the time to ask her, and I'll leave. You don't have to do it right here in front of me.

THE DEFENDANT: I think I asked her enough, you know, pertaining to --

THE COURT: All right.

All right. Ms. Koenig, are you comfortable with the representation of him so far?

MS. KOENIG: Yes, Your Honor.

THE COURT: Do you think there's anything else that Mr. Chatrie has to know before we go through this process?

MS. KOENIG: No, Your Honor.

THE COURT: All right.

Have you discussed with your attorney, Mr. Chatrie, how any sentence will be determined? Have you talked about the sentencing guidelines?

THE DEFENDANT: Yes, Your Honor.

THE COURT: And are you entirely satisfied with what your attorney has done for you? Do you believe Ms. Koenig has done all she can so that you can make an informed decision in this matter?

THE DEFENDANT: I know she did, Your Honor.

THE COURT: Good. I'm not surprised.

Do you understand, though, that the decision of whether or not to plead guilty can only be yours? It can't be that of your attorney or of anybody else that you know.

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. Now, I need to go through with you in great detail all the rights you're waiving if I take your guilty plea. And the most obvious one is your absolute right to plead not guilty and to demand the government prove its case. And you have a right to make the government prove its case whether or not you think you're guilty. Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: And do you know that when you plead guilty, you are admitting every element of the offense and that you're admitting that the government can prove them? Do you understand that?

THE DEFENDANT: Yes, ma'am.

THE COURT: So the trial rights you'd be waiving are these:

The right to see and hear all the evidence against you; the right to confront and cross-examine any witness; the right to the effective assistance of counsel at all stages, so that would include a trial; the right to use subpoenas to gather and present evidence, and you'd have the right not to present evidence. You'd have the right to a speedy public trial, during which you could testify or you could decide not to testify, and if you decided not to testify, the Judge would instruct the jury that nothing could be concluded from your remaining silent because you have a right to remain silent.

The Judge would also be sure that the jury knew that the verdict would have to be unanimous, and that the government has to prove every element of the offense.

Do you understand also that by pleading guilty, you're admitting all the essential elements of the offense, and you're waiving all these trial rights I just explained to you, and you're saying, in affect, you did this, and you can never say again you did not? Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: Are you intending to plead guilty to this charge because, in fact, you are guilty of it?

THE DEFENDANT: Yes, Your Honor.

THE COURT: Do you understand that if I take your plea, the only issue remaining in this court will be what sentence is to be imposed, and that will be made in this court by me at a later date? Do you understand that?

THE DEFENDANT: Yes, Your Honor, fully.

THE COURT: Pardon me?

THE DEFENDANT: I fully understand it.

THE COURT: Okay. Good.

Now, I do want to review the plea agreement with you. What I have is a 15-paged numbered document, and there was a place for you to have signed on page 15, Mr. Chatrie. Did you sign there?

THE DEFENDANT: Yes, Your Honor.

THE COURT: And Ms. Koenig on 15?

MS. KOENIG: Yes, Your Honor.

THE COURT: And the government on page 14?

MR. SIMON: Yes, Judge.

THE COURT: Now, I want to go over with you, Mr. Chatrie, what I think are the essential terms of the plea to make sure it agrees with what you think the deal is here.

THE DEFENDANT: Okay.

THE COURT: As I understand it, you're agreeing to waive indictment and plead guilty to the two counts that we have been talking about.

You're agreeing to plead guilty because you are guilty, and you're admitting the facts in the statement of facts and that they establish guilt.

You understand that your lawyer has rendered effective assistance of counsel. You're satisfied of that. And you know you're waiving all the trial rights that I just went over in great detail.

You're agreeing that you are pleading conditionally, and that you waive your right to challenge the conviction on direct appeal except that you are preserving the right to appeal the District Court's March 3, 2022, memorandum opinion and order denying the motion to suppress evidence obtained under the geofence warrant, ECF Nos. 220 and 221.

You understand and agree that you will pay the monetary penalties that are imposed by the Court, including restitution, which will be due immediately and subject to immediate enforcement.

You understand that you're agreeing to pay a mandatory special assessment of $100 per felony count, which is a total of $200.

You're agreeing that restitution is mandatory, and you're agreeing to the entry of a restitution order for the full amount of the victims' losses as determined by the Court.

And in paragraph 11, the victim is named as the Call Federal Credit Union, and the amount is $196,932.01.

You're agreeing that you understand that forfeiture is part of the process and you're agreeing to forfeit all interest in any robbery or firearms-related asset that you own or have had direct or indirect control over.

In paragraph 12, what is listed is a Taurus 9mm semiautomatic pistol and also $102,293 in U.S. currency seized in Richmond on August 13th of 2019.

You're agreeing to waive any interest in any administrative or judicial forfeiture proceeding, civil or criminal. You're also agreeing to waive constitutional and statutory challenges to forfeiture in any manner. And you're agreeing to fully participate in the forfeiture process, including making your financial information available.

It's understood that the failure to participate in the financial investigation as described in the plea agreement may constitute a

failure to accept responsibility under the guidelines 3E1.1. And you're agreeing to identify assets valued at more than $5,000 that have been transferred to third parties.

It's noted that by pleading guilty there may be consequences for any immigration status if you're not a citizen of the United States or for citizenship status if you are a naturalized citizen, and that includes the issues that we talked about, including an understanding that a guilty plea for a conviction of robbery of a credit union by force and use in carrying and brandishing a firearm during and in relation to a crime of violence make it such that removal is presumptively mandatory.

It is also the case if you are a naturalized citizen you acknowledge that certain convictions, which may include these convictions, may expose you to a denaturalized station under federal law.

In exchange, pursuant to 11(c)(1)(B), Federal Rule of Criminal Procedure, the United States and you are stipulating, will recommend to the Court the following provisions of the sentencing guidelines that are listed in paragraph 5 of your plea agreement. They're all under 2B3.1. And there's an agreement that the base offense level will be 20, that there

will be a two-level increase for taking property from a financial institution. There will be a four-level increase for persons abducted to facilitate commission of the offense, and a two-level increase for loss of more than $95,000.

The United States and you are agreeing that you have assisted the government in the investigation and your own misconduct by timely notifying of an intention to plead guilty. And so if you qualify for the two-level decrease in the offense level for acceptance of responsibility under 3E1.1 and your offense level is 16 or greater, the government agrees to file a motion to ask for an additional point off for acceptance of responsibility.

The United States and you are stipulating and will recommend that the Court impose no other specific offense characteristics, and will say they do not apply, and no other chapter 3 adjustments apply.

The resulting adjusted offense level for Count One is 25, criminal history category I, resulting in a guideline range of 57 to 71 months. Taken together with a consecutive of 80 months of imprisonment on Count Two, the parties agree that the appropriate advisory guideline range is 141 to 155 months' imprisonment.

The United States is agreeing that it will not argue for a sentence above 155 months' imprisonment, and you are agreeing to argue for no less than 130 months' imprisonment, which would include a motion for a downward variance. The United States is making clear it does not believe that a downward variance is appropriate.

Now, the thing you have to remember is all of that is a recommendation. It's not binding on me for purposes of sentencing.

So except for with respect to the motion to suppress, you know that you have a right to appeal the sentence. You are waiving the conviction and the sentence. You are waiving your right to appeal the conviction except as to the motion to suppress and any sentence within the statutory maximum that we have described during the process of this hearing.

The United States is agreeing that it will not further criminally prosecute you in the Eastern District of Virginia for the specific conduct in the information, the indictment, or the statement of facts, except if there is a crime of violence or conspiracy to commit or aid and abet a crime of violence not charged in the information as an offense.

The United States is agreeing that at the

appropriate time they will move to dismiss the indictment against you. They are agreeing, with respect to the paragraph about forfeiture, that they will not use any truthful and complete information provided by you for additional offenses except for any crime of violence and that, pursuant to the guidelines, no truthful information that you provide will be used in determining your applicable guideline range.

What would constitute a breach is also discussed and, that includes if you were to withdraw from the agreement or commit or attempt to commit any federal, state, or local crime, any additional one, or intentionally give materially false information, in which case the United States will be released from the obligations under the agreement, but you could not withdraw these guilty please.

Is that your understanding of the agreement here?

THE DEFENDANT: Yes, ma'am.

THE COURT: Other than that, have there been any other promises or even any threats to get you to plead guilty?

THE DEFENDANT: No, ma'am.

THE COURT: Do you understand that the

recommendations, as detailed as they are with respect to your sentencing, they aren't binding on me? Do you know that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: And do you understand that even though you've waived your right to appeal the sentence except as provided in your agreement, the United States has not waived its right to appeal? Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: So do you understand it's the Eastern District of Virginia that has agreed not to prosecute you for any non-violent offenses related to the charges that you're intending to plead guilty to, and it doesn't apply to another jurisdiction? Do you understand that?

THE DEFENDANT: Can you repeat that for me, please?

THE COURT: Ms. Koenig, do you want to talk to him?

MS. KOENIG: I do, Your Honor.

(Ms. Koenig and the defendant are conferring.)

THE DEFENDANT: Yes, I understand, Your Honor.

THE COURT: You understand it? Okay.

And do you understand with respect to forfeiture you have to provide truthful information, which can affect your acceptance of responsibility if you do not? Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: Now, I do want to go over the consent order of forfeiture with you. That's a three-page document. And there was a place for you to have signed on page 3. Did you sign there, Mr. Chatrie?

THE DEFENDANT: Yes, Your Honor.

THE COURT: And Ms. Koenig?

MS. KOENIG: Yes, Your Honor.

THE COURT: And the government on page 3?

MR. SIMON: That's correct, Judge.

THE COURT: All right. It lists in paragraph 1 a sum of money in the amount of $195,000, and in the subparagraph B, it specifically lists $102,293.00 of currency that was seized in Richmond, as we just went over, and the Taurus 9mm automatic pistol.

Now, Ms. Koenig, did you have sufficient information to review this issue with your client, forfeiture, before you came into the courtroom?

MS. KOENIG: I did, Your Honor.

THE COURT: And, Mr. Chatrie did you have a sufficient time to ask all the questions you had about that before you signed the document?

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. Now, I do want to talk about the sentencing guideline process. We're going to go through a presentence report and that will determine your recommended sentence pursuant to the Sentence Guideline Act, which involves considering all of your criminal activity even if it's not listed in the information. Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: And do you know that the Court has a series of factors that it must consider under the guidelines? It includes information about whether you accept responsibility, but includes other factors that can affect the recommended range up or down. Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. And do you know that the Court must examine your prior criminal history, if there is any, and that has an affect on the recommended range of punishment?

THE DEFENDANT: Yes, Your Honor.

THE COURT: And do you know that the

guidelines are not mandatory and a judge can impose a sentence above or below the recommended range within reason?

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. So what happens is if I accept your guilty pleas, I'll refer your case to the probation office for preparation of what's called "the presentence report," and it's through that reporting process that the guidelines would be calculated. A probation officer would speak to you, and your attorney, and the government, and would look at the guidelines, and look at your background, and these events, and then print out a report that has a recommended sentencing range within it.

I mention that because I would be very surprised if Ms. Koenig had not given you an estimate of what the guidelines might be, but even her estimate is only a prediction and no promise because that report hasn't even been started yet. Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. Do you understand that there are circumstances where a court can depart or vary upward from the recommended range?

THE DEFENDANT: Yes, Your Honor.

THE COURT: A process for that to happen must occur. And do you also understand that a court can vary downward or depart downward based on any motion? And I understand that has been preserved for you to file that motion. Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: And do you know, though, that even if it's filed, it does not have to be accepted? The Court has to review it independently and make a finding it's for a good cause.

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. Now, Ms. Koenig, are you satisfied that it's in your client's best interest to accept the terms of the plea agreement rather than to proceed to trial?

MS. KOENIG: Yes, Your Honor.

THE COURT: Are you satisfied that Mr. Chatrie fully understands the charges against him?

MS. KOENIG: I am.

THE COURT: Are you satisfied that Mr. Chatrie has been competent and fully able to cooperate with you throughout the course of this matter?

MS. KOENIG: Yes, Your Honor.

THE COURT: Are you satisfied there are no

meritorious defenses that can be raised, or if there are, that it is in his best interest to enter into the plea agreement and preserve certainly the right to appeal the motion to suppress?

MS. KOENIG: Yes, Your Honor.

THE COURT: Are you satisfied that all of your client's rights have been preserved throughout these proceedings?

MS. KOENIG: Yes, Your Honor.

THE COURT: Do you know of any reason why I should not accept a plea?

MS. KOENIG: I do not.

THE COURT: All right.

So, Mr. Chatrie, this is where I ask you how do you plead to Count One, which charges you with robbery of a credit union, in violation of 18 U.S.C. 2113(a) and (d); guilty or not guilty?

THE DEFENDANT: Guilty as charged, Your Honor.

THE COURT: All right. And how do you plead to Count Two, which charges you with using, carrying, and brandishing a firearm during and in relation to a crime of violence in violation of Title 18 U.S.C. Section 924(c)(1)(A), guilty or not guilty?

THE DEFENDANT: Guilty as charged.

THE COURT: All right. Now, sir, to make a finding as to guilt, I need to review the statement of facts with you that have been offered as part of the plea. That is a four-page document?

MS. KOENIG: Five pages, Your Honor.

THE COURT: Five-page document.

MS. KOENIG: I think there's some extra spacing on page 4.

THE COURT: Right. And there was a place for you to have signed, Mr. Chatrie, on page 5?

THE DEFENDANT: Yes, Your Honor.

THE COURT: You signed. And Ms. Koenig also?

MS. KOENIG: Yes, Your Honor.

THE COURT: And then the government on page 3?

MR. SIMON: That's correct, Judge.

THE COURT: All right. Now, I have reviewed the information in the statement of facts, and it is sufficient to support a finding of guilt, but before I do that, I want to ask you, Ms. Koenig, is there anything in these facts that you think is wrong, that should be changed, or added in, or taken out?

MS. KOENIG: No, Your Honor. We've already made any edits that needed to be made.

THE COURT: Okay. How about you,

Mr. Chatrie? Anything in these facts that you think is wrong, that should be changed, or added in, or taken out?

THE DEFENDANT: No, Your Honor.

THE COURT: Did you sign the document because the information in it is true?

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. So, sir, this is where I could make my finding of guilt, and it's your last opportunity to withdraw your guilty pleas. Are you prepared for me to go ahead and make my finding?

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. So it is the finding of the Court in the case of the *United States versus Okello T. Chatrie* that Mr. Chatrie is fully competent and capable of entering an informed plea, that he is aware of the nature of the charges and the consequences of the pleas, and that the pleas of guilty to Counts One and Two in the information are knowing and voluntary and supported by an independent basis in fact containing each of the essential elements of the offense. The pleas are therefore accepted, and Mr. Chatrie is now adjudged guilty of those offenses.

So, sir, this is where I order the probation

office to prepare your presentence report, as I indicated. And I want to be sure that you understand the scheduling order that I will enter, but Ms. Koenig is going to go over that in detail about when things are due and when events happen.

I always mention, though, a couple parts of the process because I think they're important. One is that, as I said, you'll be interviewed by a probation officer as that person prepares your presentence report. And what I want you to know is that you may have your lawyer with you during any conversation with your probation officer. Do you understand that?

THE DEFENDANT: Yes, Your Honor.

THE COURT: And I also want you to know that there's a period of time before the final presentence report is issued where you can lodge objections or try to change information in the report. And if you don't do it by the deadline, you waive it. You can't do it afterward. But the process includes a requirement that both sides speak to each other and see if they can agree to any changes. And it's only if they cannot agree that a formal motion is put in front of me, and then we have a separate hearing on that dispute. Do you understand that?

THE DEFENDANT: Understood.

THE COURT: All right. Okay. So we need to set a date. I'm going to allow you all to sit down while we do that.

MS. KOENIG: Your Honor, I wanted to ask the Court to strongly consider a sentencing date that is as soon as possible under the guideline procedure.

Mr. Chatrie has been in local custody since September of 2019 because it took a long time to litigate the important issues in the case. The defense has already prepared the mitigation that we would anticipate presenting. I have a psychological forensic evaluation that I have already provided to the government as a part of the negotiations process.

Certainly local custody is not where one wants to be for almost three years. Mr. Chatrie's -- I think his mental health issues have been dramatically exacerbated by the lengthy amount of time that the lawyers have needed in the case to present the case.

And so we all are very familiar with the facts of the case. And while the probation office does accurately need to calculate the guidelines, Mr. Chatrie doesn't have any prior criminal convictions. So it's not a matter of having to track down old records or things like that. So I am asking

the Court to strongly consider setting the sentencing as soon as we can.

THE COURT: Does the United States object to that? Have you all discussed this?

MR. SIMON: Judge, we've heard the request. We have not discussed in detail sort of recognizing that it's up to the Court and to the probation office, the probation office's resources, how close in time we can have the sentencing.

I'd only request that we consider also the need to make sure that the victims in this case can appear if they'd like to but also provide statements. So I think, you know, at least 45, 60 days would be ideal. I think regularly it's a 90-day period, but it's really going to be up to the probation office, and we'd want to make sure that they have enough time to get it done.

THE COURT: All right. All right. Well, we do have a representative from the probation office here. Mr. Zychowski, do you have any sense of a relatively quicker process that we could go through, how long it might take? So I want everybody to know that because of COVID, the probation office is stretched. And so we've actually been going out 120 days. I don't think we need that. But,

Mr. Zychowski, do you have a sense of when you might be able to do it, meaning the office, not you personally?

THE PROBATION OFFICER: Well, I will be assigned this investigation. Does the attorney have a suggested time frame?

MS. KOENIG: Your Honor, I wasn't necessarily meaning to suggest that we need to go shorter than the 75 days that's provided for the scheduling order. I definitely do not want to go past the 90 days of the scheduling order, but I think that 75 days, which includes the 35 days, for the process in terms of the presentation and objections, if there are any. But I do think that 40 days, given the fact that this Court has authored very extensive factual opinions in this case about the facts that aid Mr. Zychowski, I think, greatly in not having to go through voluminous discovery, as well as not having a criminal history, and I can give Mr. Zychowski the forensic psychological evaluation. That would hopefully aid us to be able to get to about 75 days.

THE COURT: All right. Does that sound possible to you, Mr. Zychowski? There is an extensive record here that ultimately has resulted in findings of fact, and an opinion, too, really, so it is the

case that you would have more of a start maybe than in most cases.

THE PROBATION OFFICER: A head start, yes. The only delay that I would anticipate is verifying personal information because we don't get a lot of that information until we interview the defendant because of the jail's schedule to do an interview. But I think she had already foreseen that.

MS. KOENIG: Yes. And I'm laughing a little bit because Mr. Zychowski has to track me down sometimes to pin down some availability where I can block out a couple of hours of time. But I will promise Mr. Zychowski, I will promise to the Court, I will promise to Mr. Chatrie and the government that I will make myself available to do those interviews in a speedy manner.

THE COURT: And you'll help him make sure that the facility makes Mr. Chatrie available; is that correct?

MS. KOENIG: I'll do my very best, Your Honor, yes.

THE COURT: All right. So I'll tell you both that if you're having problems with the facility, I am happy to do whatever it is I can within my power to make them make Mr. Chatrie available. All right?

THE PROBATION OFFICER: Thank you, Judge. I just want to point out, it's not -- it's never her delay. It is the jail's limited schedule given the video technology equipment that they have. So it's more of a delay getting that scheduled than her personally.

THE COURT: Right. It was good of her to fall on her sword, but I know that it's been difficult, in any event.

So, does somebody know when 75 days is? I may.

MS. KOENIG: Your Honor, that would put us about July 23, which is a Saturday. So that won't work. So maybe the following week.

Mr. Simon is indicating that he is not available that week but perhaps the week of August 1st.

THE COURT: How about the August 2nd?

MR. SIMON: That works for us, Judge.

MS. KOENIG: That works for the defense, Your Honor.

THE COURT: All right. Are we going to have witnesses, do you think?

MR. SIMON: We don't intend at this time to have witnesses but would leave time open possibly.

We're going to talk to folks, and we may need to put on some evidence.

THE COURT: All right. Well, how about I set it for 11 o'clock so we have time to have evidence or argument?

MS. KOENIG: Thank you, Your Honor.

THE COURT: All right. I am going to find that the waiver of indictment and the consent order of forfeiture are knowingly and voluntarily signed and, as to indictment, waived. So we'll enter those on the record.

All right. Is there anything else that we need to cover?

MR. SIMON: Nothing further from the United States, Judge.

MS. KOENIG: No, Your Honor. Thank you.

THE COURT: And, Mr. Zychowski, I appreciate your making yourself available. And certainly we will all -- this group I know will work together to make sure we can get things done as quickly as possible.

THE PROBATION OFFICER: Thank you, Your Honor.

THE COURT: So, Mr. Chatrie, I will see you on August 2nd at 11 o'clock. In the meantime, you will be held under the same conditions under which you

have been held. And I encourage you to stay in close contact with Ms. Koenig so the presentence report process can be as accurate and as quick as possible. All right?

THE DEFENDANT: Thank you, Your Honor.

THE COURT: Thank you. All right. We can call court.

(The proceedings were adjourned at 3:15 p.m.)

I, Diane J. Daffron, certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/s/

_____ _____

DIANE J. DAFFRON, RPR, CCR DATE

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA v. OKELLO T. CHATRIE, Defendant.	No. 3:19-cr-130-MHL

PLEA AGREEMENT

Jessica D. Aber, United States Attorney for the Eastern District of Virginia; undersigned counsel for the United States; the defendant, Okello T. Chatrie; and the defendant's counsel have entered into an agreement pursuant to Rule 11 of the Federal Rules of Criminal Procedure. The terms of this Plea Agreement are as follows:

1. Offense and Maximum Penalties

The defendant agrees to waive indictment and plead guilty to Counts One and Two of the Criminal Information. Count One charges the defendant with Robbery of a Credit Union, in violation of 18 U.S.C. §§ 2113(a), (d). The maximum penalties for this offense are a term of 25 years of imprisonment, a fine of $250,000, full restitution as outlined below, forfeiture of assets as outlined below, a special assessment pursuant to 18 U.S.C. § 3013, and a supervised release term of 3 years. Count Two charges the defendant with Using, Carrying, and Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A). The penalties for this offense are a mandatory minimum term of imprisonment of 7 years and a maximum term of life imprisonment, a fine of $250,000, full restitution as outlined below, forfeiture of assets as outlined below, a special assessment pursuant to 18 U.S.C. § 3013, and a supervised release term of 5 years.

The defendant understands that any supervised release term is in addition to any prison term the defendant may receive, and that a violation of a term of supervised release could result in the defendant being returned to prison for the full term of supervised release.

2. Detention Pending Sentencing

The defendant understands that this case is governed by 18 U.S.C. §§ 3143(a)(2) and 3145(c). These provisions provide that a judicial officer shall order that a person who has been found guilty of an offense of this kind be detained unless there are statutory justifications why such person's detention would not be appropriate.

3. Factual Basis for the Plea

The defendant will plead guilty because the defendant is in fact guilty of the charged offenses. The defendant admits the facts set forth in the Statement of Facts filed with this Plea Agreement and agrees that those facts establish guilt of the offenses charged beyond a reasonable doubt. The Statement of Facts, which is hereby incorporated into this Plea Agreement, constitutes a stipulation of facts for purposes of Section 1B1.2(c) of the Sentencing Guidelines.

4. Assistance and Advice of Counsel

The defendant is satisfied that the defendant's attorney has rendered effective assistance. The defendant understands that by entering into this Plea Agreement, defendant surrenders certain rights as provided in this agreement. The defendant understands that the rights of criminal defendants include the following:

a. the right to plead not guilty and to persist in that plea;

b. the right to a jury trial;

c. the right to be represented by counsel—and, if necessary, have the court appoint counsel—at trial and at every other stage of the proceedings; and

d. the right at trial to confront and cross-examine adverse witnesses, to be protected from compelled self-incrimination, to testify and present evidence, and to compel the attendance of witnesses.

5. Sentencing Guidelines, Recommendations, and Roles

The defendant understands that the Court has jurisdiction and authority to impose any sentence within the statutory maximum described above, but that the Court will determine the defendant's actual sentence in accordance with 18 U.S.C. § 3553(a). The defendant understands that the Court has not yet determined a sentence and that any estimate of the advisory sentencing range under the U.S. Sentencing Commission's Sentencing Guidelines Manual the defendant may have received from the defendant's counsel, the United States, or the Probation Office, is a prediction, not a promise, and is not binding on the United States, the Probation Office, or the Court. Additionally, pursuant to the Supreme Court's decision in *United States v. Booker*, 543 U.S. 220 (2005), the Court, after considering the factors set forth in 18 U.S.C. § 3553(a), may impose a sentence above or below the advisory sentencing range, subject only to review by higher courts for reasonableness. The United States makes no promise or representation concerning what sentence the defendant will receive, and the defendant cannot withdraw a guilty plea based upon the actual sentence.

Further, in accordance with Federal Rule of Criminal Procedure 11(c)(1)(B), the United States and the defendant stipulate and will recommend to the Court that the following provisions of the Sentencing Guidelines apply:

Guideline(s)	**Description**	Offense Level
§ 2B3.1(a)	Base offense level	+20
§ 2B3.1(b)(1)	Taking Property from a Financial Institution	+2
§ 2B3.1(b)(4)	Persons Abducted to Facilitate Commission of Offense	+4
§ 2B3.1(b)(7)(C)	Loss of more than $95,000	+2

The United States and the defendant further agree that the defendant has assisted the government in the investigation and prosecution of the defendant's own misconduct by timely notifying authorities of the defendant's intention to enter a plea of guilty, thereby permitting the government to avoid preparing for trial and permitting the government and the Court to allocate their resources efficiently. If the defendant qualifies for a two-level decrease in offense level pursuant to U.S.S.G. § 3E1.1(a) and the offense level prior to the operation of that section is a level 16 or greater, the government agrees to file, pursuant to U.S.S.G. § 3E1.1(b), a motion prior to, or at the time of, sentencing for an additional one-level decrease in the defendant's offense level.

Further, in accordance with Federal Rule of Criminal Procedure 11(c)(1)(B), the United States and the defendant stipulate and will recommend to the Court that no other specific offense characteristics apply and no other Chapter 3 adjustments apply. The resulting adjusted offense level for Count One is 25, criminal history category I, resulting in a guideline range of 57-71 months. Taken together with the consecutive sentence of 84 months' imprisonment on Count Two, the parties agree that the appropriate advisory guideline range is 141-155 months' imprisonment. Moreover, pursuant to this agreement, the United States will not argue for a sentence above 155 months' imprisonment, and the defendant agrees to argue for no less than 130 months' imprisonment, which would include a motion for a downward variance. To be clear, the United States does not agree that any downward variance is appropriate here, and these agreements are not binding on the Court.

The United States and the defendant have not agreed on any further sentencing issues, whether related to the Sentencing Guidelines or the factors listed in 18 U.S.C. § 3553(a), other than those set forth above or elsewhere in this Plea Agreement. Any stipulation on a Guidelines

provision does not limit the parties' arguments as to any other Guidelines provisions or sentencing factors under Section 3553(a), including arguments for a sentence within or outside the advisory Guidelines range found by the Court at sentencing.

6. Preservation of Appeal, FOIA, and Privacy Act Rights

The defendant agrees that he is pleading guilty conditionally. The defendant waives his right to challenge his conviction on direct appeal except that, pursuant to Federal Rule of Criminal Procedure 11(a)(2), the defendant preserves his right to appeal the District Court's March 3, 2022 Memorandum Opinion and Order denying the defendant's Motion to Suppress Evidence obtained under the Geofence Warrant (ECF Nos. 220, 221).

The defendant also understands that 18 U.S.C. § 3742 affords a defendant the right to appeal the sentence imposed. Nonetheless, the defendant knowingly waives the right to appeal the conviction, except as noted above, and any sentence within the statutory maximum described above (or the manner in which that sentence was determined) on the grounds set forth in 18 U.S.C. § 3742 or on any ground whatsoever other than an ineffective assistance of counsel claim that is cognizable on direct appeal, in exchange for the concessions made by the United States in this Plea Agreement. This agreement does not affect the rights or obligations of the United States as set forth in 18 U.S.C. § 3742(b). The defendant also hereby waives all rights, whether asserted directly or by a representative, to request or receive from any department or agency of the United States any records pertaining to the investigation or prosecution of this case, including without limitation any records that may be sought under the Freedom of Information Act, 5 U.S.C. § 552, or the Privacy Act, 5 U.S.C. § 552a.

7. Immunity from Further Prosecution in This District

The United States will not further criminally prosecute the defendant in the Eastern District of Virginia for the specific conduct described in the Information, Indictment, and Statement of Facts, except that the United States may prosecute the defendant for any crime of violence or conspiracy to commit, or aiding and abetting, a crime of violence not charged in the Information, Indictment, and as an offense. In such a prosecution, the United States may allege and prove conduct described in the Information, Indictment, and or Statement of Facts. "Crime of violence" has the meaning set forth in 18 U.S.C. § 16.

8. Dismissal of Other Counts

As a condition of the execution of this agreement and the Court's acceptance of the defendant's plea of guilty, the United States will move to dismiss the Indictment against this defendant at the conclusion of this defendant's sentencing hearing.

9. Payment of Monetary Penalties

The defendant understands and agrees that, pursuant to 18 U.S.C. § 3613 and 18 U.S.C. § 3572, all monetary penalties imposed by the Court, including restitution, will be due immediately and subject to immediate enforcement by the United States as provided for in Section 3613. If the Court imposes a schedule of payments, the defendant understands that the schedule of payments is merely a minimum schedule of payments and not the only method, nor a limitation on the methods, available to the United States to enforce the judgment. Until all monetary penalties are paid in full, the defendant will be referred to the Treasury Offset Program so that any federal payment or transfer of returned property to the defendant will be offset and applied to pay the defendant's unpaid monetary penalties. If the defendant is incarcerated, the defendant agrees to participate voluntarily in the Bureau of Prisons' Inmate Financial

Responsibility Program, regardless of whether the Court specifically directs participation or imposes a schedule of payments. Defendant agrees to make good-faith efforts toward payment of all monetary penalties imposed by the Court.

10. Special Assessment

Before sentencing in this case, the defendant agrees to pay a mandatory special assessment of $100 per felony count of conviction, pursuant to 18 U.S.C. § 3013(a)(2)(A).

11. Restitution

The defendant agrees that restitution is mandatory pursuant to 18 U.S.C. § 3663A(c)(1), and the defendant agrees to the entry of a Restitution Order for the full amount of the victims' losses as determined by the Court. Pursuant to 18 U.S.C. § 3663A(c)(2), the defendant further agrees that an offense listed in Section 3663A(c)(1) gave rise to this Plea Agreement and, as such, victims of the conduct described in the charging instrument, Statement of Facts, or any related or similar conduct shall be entitled to restitution. Without limiting the amount of restitution that the Court must impose, the parties agree that, at a minimum, the following victims have suffered the losses identified below and are entitled to restitution:

Victim Name and Address	Restitution Amount
Call Federal Credit Union 3640 Call Federal Drive, Midlothian, Virginia 23112	$196,932.01

The defendant understands that forfeiture and restitution are separate and distinct financial obligations that must be imposed upon a criminal defendant. The defendant further understands that restitution will be enforced pursuant to 18 U.S.C. § 3572, 18 U.S.C. § 3613, and 18 U.S.C. § 3664(m).

12. Forfeiture Agreement

The defendant understands that the forfeiture of assets is part of the sentence that must be imposed in this case. The defendant agrees to forfeit all interests in any robbery or firearms-related asset that the defendant owns or over which the defendant exercises control, directly or indirectly. This includes any property that is traceable to, derived from, fungible with, or a substitute for the following: proceeds of the offense and any firearm or ammunition used in or involved in the offense. The defendant agrees that the assets subject to forfeiture include, but are not limited to, the following specific property:

a. Taurus G2C, 9mm semi-automatic pistol, bearing serial number TLW87541

b. $102,293 in U.S. Currency seized in Richmond, Virginia on August 13, 2019

The defendant understands that if the assets subject to forfeiture are not available to the United States to be forfeited, the Court must enter a forfeiture money judgment in the amount of the unavailable assets. *United States v. Blackman*, 746 F.3d 137 (4th Cir. 2014).

The defendant further agrees to waive all interest in the asset(s) in any administrative or judicial forfeiture proceeding, whether criminal or civil, state or federal. The defendant agrees to consent to the entry of orders of forfeiture for such property and waives the requirements of Federal Rules of Criminal Procedure 32.2 and 43(a) regarding notice of the forfeiture in the charging instrument, announcement of the forfeiture at sentencing, and incorporation of the forfeiture in the judgment. Defendant admits and agrees that the conduct described in the charging instrument and Statement of Facts provides a sufficient factual and statutory basis for the forfeiture of the property sought by the government.

13. Waiver of Further Review of Forfeiture

The defendant further agrees to waive all constitutional and statutory challenges to forfeiture in any manner (including direct appeal, habeas corpus, or any other means) to any forfeiture carried out in accordance with this Plea Agreement on any grounds, including that the forfeiture constitutes an excessive fine or punishment. The defendant also waives any failure by the Court to advise the defendant of any applicable forfeiture at the time the guilty plea is accepted as required by Rule 11(b)(1)(J). The defendant agrees to take all steps as requested by the United States to pass clear title to forfeitable assets to the United States, and to testify truthfully in any judicial forfeiture proceeding. The defendant understands and agrees that all property covered by this agreement is subject to forfeiture as proceeds of the offense and property used or involved in the offenses.

14. The Defendant's Obligations Regarding Assets and Financial Investigation

The defendant agrees to fully participate in the United States' pre- and post-judgment financial investigation. Such participation includes the identification of assets in which the defendant has any legal or equitable interest to determine what assets may be available for payment to restitution, forfeiture, and/or any fine imposed in this case. The defendant agrees that the defendant's financial information is subject to investigation and disclosure pre-judgment to the same extent as financial information will be subject to discovery after judgment is imposed. The defendant understands that 31 U.S.C. § 3711(h)(1) permits the United States to obtain the defendant's credit report after sentencing and expressly authorizes the United States to obtain the defendant's credit report prior to sentencing in this case. The defendant understands that the United States has sole discretion over whether it will obtain defendant's credit report pursuant to this Plea Agreement. If the United States determines that it will obtain defendant's credit report

prior to sentencing pursuant to this Plea Agreement, the defendant authorizes the United States, and the United States agrees, to provide a copy to defense counsel upon request. The defendant understands that failure to participate in the financial investigation as described in this paragraph may constitute the defendant's failure to accept responsibility under U.S.S.G § 3E1.1.

Within 14 days of a request by the United States, or other deadline agreed upon by the parties, the defendant agrees to provide all information about all of the defendant's assets and financial interests to the United States and the Probation Office and, if requested, submit to a debtor's examination, complete a financial disclosure statement under penalty of perjury, and/or undergo any polygraph examination the United States may choose to administer concerning such assets and financial interests. The defendant also agrees to provide or consent to the release of the defendant's tax returns for the previous five years. The defendant understands that assets and financial interests subject to disclosure include assets owned or held directly or indirectly, individually or jointly, in which the defendant has any legal interests, regardless of title, including any interest held or owned under any other name, trusts, and/or business entities presently and since date of the first offense giving rise to this Plea Agreement, or giving rise to the charges presently pending against the defendant, whichever is earlier.

The defendant shall identify all assets valued at more than $5,000 that have been transferred to third parties since the date of the first offense giving rise to this Plea Agreement, including the location of the assets and the identities of third parties to whom they were transferred. The defendant agrees not to transfer any assets valued at more than $5,000 without approval of the Asset Recovery Unit of the U.S. Attorney's Office until the fine, forfeiture, and restitution ordered by the Court at sentencing are paid in full or otherwise terminated by operation of law. The defendant agrees to take all steps requested by the United States to obtain

from any other parties by any lawful means any records of assets contemplated by this paragraph in which the defendant has or had an interest. Until the fine, forfeiture, and restitution ordered by the Court are paid in full or otherwise terminated by operation of law, the defendant agrees to notify the Asset Recovery Unit of the U.S. Attorney's Office of a change in address within 30 days of such change.

The United States will not use any truthful and complete information provided by the defendant pursuant to this paragraph for additional criminal offenses against the defendant in the Eastern District of Virginia, except in any prosecution for a crime of violence or conspiracy to commit, or aiding and abetting, a crime of violence (as defined in 18 U.S.C. § 16). Pursuant to U.S.S.G. § 1B1.8, no truthful information that the defendant provides pursuant to defendant's obligations under this paragraph will be used in determining the applicable guideline range, except as provided in Section 1B1.8(b). Nothing in this agreement, however, restricts the Court's or Probation Officer's access to information and records in the possession of the United States. Furthermore, nothing in this agreement prevents the United States in any way from prosecuting the defendant should the defendant knowingly provide false, untruthful, or perjurious information or testimony, or from using information provided by the defendant in furtherance of any forfeiture action or restitution enforcement action, whether criminal or civil, administrative or judicial.

15. Impact of Guilty Plea on Immigration or Citizenship Status

The defendant recognizes that pleading guilty may have consequences for defendant's immigration status, if defendant is not a citizen of the United States, or for defendant's citizenship status, if defendant is a naturalized citizen. Under federal law, a broad range of crimes are removable offenses, including offenses that qualify as aggravated felonies, crimes

involving moral turpitude, and conduct involving controlled substances and firearms, among many other categories of criminal activity. Indeed, if defendant is not a citizen of the United States, defendant's guilty plea to and conviction for Robbery of a Credit Union by Force and Using, Carrying, and Brandishing a Firearm During and in Relation to a Crime of Violence make it such that removal is presumptively mandatory. Likewise, if defendant is a naturalized citizen, defendant acknowledges that certain convictions, which may include defendant's conviction, may expose defendant to denaturalization under federal law. Because removal, denaturalization, and other immigration consequences are the subjects of a separate proceeding, defendant understands that no one, including defendant's attorney, the U.S. Attorney's Office, or the U.S. District Court, can predict to a certainty the effect of defendant's conviction on defendant's immigration or citizenship status. Defendant nevertheless affirms that defendant knowingly and voluntarily agrees to plead guilty regardless of any present or future immigration consequences that defendant's plea may entail, even if the consequence is defendant's automatic removal from the United States or denaturalization followed by automatic removal from the United States.

16. Breach of the Plea Agreement and Remedies

This Plea Agreement is effective when signed by the defendant, the defendant's attorney, and an attorney for the United States. The defendant agrees to entry of this Plea Agreement at the date and time scheduled with the Court by the United States (in consultation with the defendant's attorney). If the defendant withdraws from this agreement, or commits or attempts to commit any additional federal, state, or local crimes, or intentionally gives materially false, incomplete, or misleading testimony or information, or otherwise violates any provision of this agreement, then:

a. The United States will be released from its obligations under this agreement. The defendant, however, may not withdraw the guilty plea entered pursuant to this agreement.

b. The defendant will be subject to prosecution for any federal criminal violation, including, but not limited to, perjury and obstruction of justice, that is not time-barred by the applicable statute of limitations on the date this agreement is signed. Notwithstanding the subsequent expiration of the statute of limitations, in any such prosecution, the defendant agrees to waive any statute-of-limitations defense.

c. Any prosecution, including the prosecution that is the subject of this agreement, may be premised upon any information provided, or statements made, by the defendant, and all such information, statements, and leads derived therefrom may be used against the defendant. The defendant waives any right to claim that statements made before or after the date of this agreement, including the Statement of Facts accompanying this agreement or adopted by the defendant and any other statements made pursuant to this or any other agreement with the United States, should be excluded or suppressed under Fed. R. Evid. 410, Fed. R. Crim. P. 11(f), the Sentencing Guidelines, or any other provision of the Constitution or federal law.

Any alleged breach of this agreement by either party shall be determined by the Court in an appropriate proceeding at which the defendant's disclosures and documentary evidence shall be admissible and at which the moving party shall be required to establish a breach of this Plea Agreement by a preponderance of the evidence.

17. Nature of the Agreement and Modifications

This written agreement constitutes the complete plea agreement between the United States, the defendant, and the defendant's counsel. The defendant and the defendant's attorney acknowledge that no threats, promises, or representations have been made, nor agreements reached, other than those set forth in writing in this Plea Agreement or any associated documents filed with the Court, to cause the defendant to plead guilty. Any modification of this Plea

Agreement shall be valid only as set forth in writing in a supplemental or revised plea agreement signed by all parties.

Jessica D. Aber
United States Attorney

By: _____
Kenneth R. Simon, Jr.
Assistant United States Attorney

By: _____
Peter S. Duffey
Assistant United States Attorney

Defendant's Signature: I hereby agree that I have consulted with my attorney and fully understand all rights with respect to the pending criminal Information, Indictment, and. Further, I fully understand all rights with respect to 18 U.S.C. § 3553 and the provisions of the Sentencing Guidelines Manual that may apply in my case. I have read this Plea Agreement and carefully reviewed every part of it with my attorney. I understand this agreement and voluntarily agree to it.

Date: 5/9/22 OChatrie

Okello T. Chatrie
Defendant

Defense Counsel's Signature: I am counsel for the defendant in this case. I have fully explained to the defendant the defendant's rights with respect to the pending Information, Indictment, and. Further, I have reviewed 18 U.S.C. § 3553 and the Sentencing Guidelines Manual, and I have fully explained to the defendant the provisions that may apply in this case. I have carefully reviewed every part of this Plea Agreement with the defendant. To my knowledge, the defendant's decision to enter into this agreement is an informed and voluntary one.

Date: 5/9/22

Laura Koenig
Counsel for the Defendant

U. S. DEPARTMENT OF JUSTICE
Statement of Special Assessment Account

This statement reflects your Special Assessment only. There may be other penalties imposed at sentencing.

ACCOUNT INFORMATION	
CRIM. ACTION NO.:	3:19-cr-130-MHL
DEFENDANT'S NAME:	Okello T. Chatrie Defendant
PAY THIS AMOUNT:	$200.00

INSTRUCTIONS:

1. **MAKE CHECK OR MONEY ORDER PAYABLE TO:**

   CLERK, U.S. DISTRICT COURT

2. **PAYMENT MUST REACH THE CLERK'S OFFICE BEFORE YOUR SENTENCING DATE.**

3. **PAYMENT SHOULD BE SENT TO:**

	In-Person (9 AM to 4 PM)	By Mail:
Alexandria Cases:	**Clerk, U.S. District Court 401 Courthouse Square Alexandria, VA 22314**	
Richmond Cases:	**Clerk, U.S. District Court 701 East Broad Street, Suite 3000 Richmond, VA 23219**	
Newport News Cases:	**Clerk, U.S. District Court 2400 West Ave., Suite 100 Newport News, VA 23607**	
Norfolk Cases:	**Clerk, U.S. District Court 600 Granby Street Norfolk, VA 23510**	

4. **INCLUDE DEFENDANT'S NAME ON CHECK OR MONEY ORDER.**

5. **ENCLOSE THIS COUPON TO ENSURE PROPER AND PROMPT APPLICATION OF PAYMENT.**

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA v. OKELLO T. CHATRIE, Defendant.	Criminal No. 3:19-cr-130-MHL

STATEMENT OF FACTS

The United States and the defendant agree that the factual allegations contained in this Statement of Facts and in Counts One and Two of the Criminal Information are true and correct, and that the United States could have proven them beyond a reasonable doubt.

1. On or about May 20, 2019, in the Eastern District of Virginia, the defendant, OKELLO T. CHATRIE, by force, violence, and intimidation, did take from the person and presence of another, namely J.W. and K.C., employees of the Call Federal Credit Union located at 3640 Call Federal Drive, Midlothian, Virginia, 23112, approximately $195,000 in United States currency, belonging to, and in the care, custody, control, management and possession of the Call Federal Credit Union, the accounts of which were then insured by the National Credit Union Administration Board, and in committing such offense, the defendant, OKELLO T. CHATRIE, did put in jeopardy the life of another person by the use of a dangerous weapon, that is a firearm, in violation of Title 18, United States Code, Sections 2113(a) and 2113(d)).

2. On or about May 20, 2019, in the Eastern District of Virginia, the defendant, OKELLO T. CHATRIE, did knowingly and unlawfully use, carry, and brandish a firearm during

and in relation to a crime of violence for which he may be prosecuted in a court of the United States, that is, credit union robbery by force and violence, and intimidation, as charged in Count One of the Criminal Information, which is re-alleged as if fully set forth here, in violation of Title 18, United States Code, Sections 924(c)(1)(A)(i) and (ii).

3. At approximately 4:50 p.m. eastern standard time, on May 20, 2019, CHATRIE entered the Call Federal Credit Union in Midlothian, Virginia, with a firearm. While CHATRIE stood in line, victim-teller J.B. asked another teller, J.W., to assist CHATRIE when he reached the counter.

4. When CHATRIE reached J.W.'s station, he presented a handwritten note. That note read, in part, "I got your family as hostage and I know where you live, If you or your coworker alert the cops or anyone your family and you are going to be hurt . . . I need at least 100k." After J.W. told him that she did not have access to that amount of money, CHATRIE pulled out a silver and black handgun. Waving the firearm around, he then directed J.W., other Call Federal Credit Union employees, and customers to move to the center of the lobby and get on the floor. Once there, CHATRIE led victims behind the teller counter and into a back room where the Credit Union's safe was located.

5. Once in the back room, CHATRIE ordered everyone to their knees at gunpoint and demanded that the bank manager open the safe. The Credit Union manager, fearing for his life, obliged by opening the safe and handing over $195,000 in United States currency.

6. Additional investigation by law enforcement revealed that CHATRIE purchased a silver and black 9mm G2C Taurus semiautomatic pistol, bearing serial number TLW87541, on April 29, 2019, at Bob Moates Sports Shop, Inc., 10418 Hull Street Rd, Midlothian, VA 23112.

7. Upon assessing location information associated with CHATRIE's Google account

obtained pursuant to a GeoFence warrant, law enforcement determined that CHATRIE's travel on May 20, 2019, showed that CHATRIE: (1) was near the church prior to the robbery at the same time that the church witness recalled seeing the suspicious individual; (2) inside the credit union during the robbery; and (3) immediately left the area following the robbery via the area near the church.

8. On August 12, 2019, law enforcement sought and obtained a federal search warrant for the residences located at XXXX Mason Dale Drive and XXXX Willis Street. When executing these search warrants in the early morning of August 13, 2019, law enforcement recovered evidence of value related to the Call Federal Credit Union robbery from XXXX Mason Dale Drive and XXXX Willis Street. At the XXXX Mason Dale Drive residence, law enforcement recovered two robbery-style demand notes from the bedroom belonging to the defendant. At XXXX Willis Street, law enforcement recovered nearly $100,000 in United States Currency (including bills wrapped in bands signed by the victim-bank teller), a silver and black Taurus G2C, 9mm semi-automatic pistol, bearing serial number TLW87541, a money counter, and a safe.

9. After being placed under arrest and advised of his *Miranda* rights, CHATRIE admitted to the armed robbery of the Call Federal Credit Union on May 20, 2019, and admitted to using the Taurus G2C, 9mm semi-automatic pistol, bearing serial number TLW87541 during the May 20, 2019 armed robbery.

JESSICA D. ABER
United States Attorney

By: _____
Kenneth R. Simon, Jr.
Peter S. Duffey

Assistant United States Attorneys

I have consulted with my counsel regarding this Statement of Facts. I knowingly and voluntarily agree that each of the above-recited facts is true and correct and that had this matter gone to trial the United States could have proven each one beyond a reasonable doubt.

5/9/22
Date

Okello T. Chatrie
Defendant

I am counsel for defendant, Okello T. Chatrie. I have carefully reviewed this Statement of Facts with him and, to my knowledge, his decision to agree to this Statement of Facts is an informed and voluntary decision.

5/9/22
Date

Laura Koenig
Counsel for Defendant

AO 245B (Rev. 09/19) (VAE 01/22) Judgment in a Criminal Case
Sheet 1

UNITED STATES DISTRICT COURT
Eastern District of Virginia
Richmond Division

UNITED STATES OF AMERICA
v.
OKELLO T. CHATRIE,
Defendant.

JUDGMENT IN A CRIMINAL CASE

Case Number: 3:19CR00130-001

USM Number: 93789-083

Defendant's Attorney: Laura J. Koenig, Esq.

The defendant pleaded guilty to Counts 1 and 2 of the Criminal Information. The defendant is adjudged guilty of these offenses:

Title and Section	Nature of Offense	Offense Ended	Count
18 U.S.C. § 2113(a) and 2113(d)	ARMED CREDIT UNION ROBBERY	5/20/2019	1
18 U.S.C. § 924(c)(1)(A)(i) and (ii)	USE, CARRY, AND BRANDISH A FIREARM DURING AN IN RELATION TO A CRIME OF VIOLENCE	5/20/2019	2

The defendant is sentenced as provided in pages 2 through 7 of this Judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

The Indictment is dismissed on the motion of the United States.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States attorney of material changes in economic circumstances.

August 10, 2022
Date of Imposition of Judgment

/s/ MHL
Signature of Judge

M. Hannah Lauck, United States District Judge
Name and Title of Judge

8-19-2022
Date

Case Number: **3:19CR00130-001**
Defendant's Name: **CHATRIE, OKELLO T.**

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a term of **ONE HUNDRED FORTY-ONE (141) MONTHS.** This terms consists of FIFTY-SEVEN (57) MONTHS on Count 1 and EIGHTY-FOUR (84) MONTHS on Count 2, to be served consecutively. The defendant shall receive credit for time served on these charges.

The Court makes the following recommendations to the Bureau of Prisons:

1. The defendant shall receive mental health treatment while incarcerated, with a focus on trauma;
2. The defendant shall receive substance abuse treatment while incarcerated if he volunteers and qualifies for it;
3. The defendant shall participate in a General Educational Development (GED) program while incarcerated;
4. Designate the defendant to FCI Fort Dix; if this facility is not available, designate the defendant to FCI Petersburg.

The court makes the following recommendations to the Bureau of Prisons:

☒ The defendant is remanded to the custody of the United States Marshal.

RETURN

I have executed this judgment as follows: _____

_____

Defendant delivered on _____ to _____

at _____, with a certified copy of this Judgment.

_____
UNITED STATES MARSHAL

By _____
DEPUTY UNITED STATES MARSHAL

Case Number: 3:19CR00130-001
Defendant's Name: CHATRIE, OKELLO T.

SUPERVISED RELEASE

Upon release from imprisonment, you will be on supervised release for a term of **THREE (3) YEARS.** This term consists of THREE (3) YEARS on each of Counts 1 and 2, to be served concurrently.

MANDATORY CONDITIONS

1. You must not commit another federal, state or local crime.
2. You must not unlawfully possess a controlled substance.
3. You must refrain from any unlawful use of a controlled substance. You must submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.
   ☐ The above drug testing condition is suspended, based on the court's determination that you pose a low risk of future substance abuse. *(check if applicable)*
4. ☒ You must make restitution in accordance with 18 U.S.C. §§ 3663 and 3663A or any other statute authorizing a sentence of restitution. *(check if applicable)*
5. ☐ You must cooperate in the collection of DNA as directed by the probation officer. *(check if applicable)*
6. ☐ You must comply with the requirements of the Sex Offender Registration and Notification Act (34 U.S.C. § 20901, et seq.) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in the location where you reside, work, are a student, or were convicted of a qualifying offense. *(check if applicable)*
7. ☐ You must participate in an approved program for domestic violence. *(check if applicable)*

You must comply with the standard conditions that have been adopted by this court as well as with any other conditions on the attached page.

Case Number: 3:19CR00130-001
Defendant's Name: CHATRIE, OKELLO T.

STANDARD CONDITIONS OF SUPERVISION

As part of your supervised release, you must comply with the following standard conditions of supervision. These conditions are imposed because they establish the basic expectations for your behavior while on supervision and identify the minimum tools needed by probation officers to keep informed, report to the court about, and bring about improvements in your conduct and condition.

1. You must report to the probation office in the federal judicial district where you are authorized to reside within 72 hours of your release from imprisonment, unless the probation officer instructs you to report to a different probation office or within a different time frame.
2. After initially reporting to the probation office, you will receive instructions from the court or the probation officer about how and when you must report to the probation officer, and you must report to the probation officer as instructed.
3. You must not knowingly leave the federal judicial district where you are authorized to reside without first getting permission from the court or the probation officer.
4. You must answer truthfully the questions asked by your probation officer.
5. You must live at a place approved by the probation officer. If you plan to change where you live or anything about your living arrangements (such as the people you live with), you must notify the probation officer at least 10 days before the change. If notifying the probation officer in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.
6. You must allow the probation officer to visit you at any time at your home or elsewhere, and you must permit the probation officer to take any items prohibited by the conditions of your supervision that he or she observes in plain view.
7. You must work full time (at least 30 hours per week) at a lawful type of employment, unless the probation officer excuses you from doing so. If you do not have full-time employment you must try to find full-time employment, unless the probation officer excuses you from doing so. If you plan to change where you work or anything about your work (such as your position or your job responsibilities), you must notify the probation officer at least 10 days before the change. If notifying the probation officer at least 10 days in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.
8. You must not communicate or interact with someone you know is engaged in criminal activity. If you know someone has been convicted of a felony, you must not knowingly communicate or interact with that person without first getting the permission of the probation officer.
9. If you are arrested or questioned by a law enforcement officer, you must notify the probation officer within 72 hours.
10. You must not own, possess, or have access to a firearm, ammunition, destructive device, or dangerous weapon (i.e., anything that was designed, or was modified for, the specific purpose of causing bodily injury or death to another person such as nunchakus or tasers).
11. You must not act or make any agreement with a law enforcement agency to act as a confidential human source or informant without first getting the permission of the court.
12. If the probation officer determines that you pose a risk to another person (including an organization), the probation officer may require you to notify the person about the risk and you must comply with that instruction. The probation officer may contact the person and confirm that you have notified the person about the risk.
13. You must follow the instructions of the probation officer related to the conditions of supervision.

U.S. Probation Office Use Only

A U.S. probation officer has instructed me on the conditions specified by the court and has provided me with a written copy of this judgment containing these conditions. For further information regarding these conditions, see *Overview of Probation and Supervised Release Conditions*, available at: www.uscourts.gov

Defendant's Signature _____ Date

Case Number: 3:19CR00130-001
Defendant's Name: CHATRIE, OKELLO T.

SPECIAL CONDITIONS OF SUPERVISION

1. Upon completion of his term of imprisonment, the defendant is to be surrendered to a duly-authorized immigration official of the Department of Homeland Security, United States Immigration and Customs Enforcement for a deportation review in accordance with established procedures provided by the Immigration and Naturalization Act, 8 U.S.C. § 1101 et seq. As a further condition of supervised release, if ordered deported, the defendant shall not enter the United States unless granted permission by the Secretary of Homeland Security.

2. The defendant shall provide the probation officer access to any requested financial information.

3. The defendant shall not incur new credit charges or open additional lines of credit without the approval of the probation officer.

4. The defendant shall apply all monies received from income tax refunds, lottery winnings, inheritances, judgments, settlements, and any anticipated or unexpected financial gains to the outstanding court-ordered financial obligation, or in a lesser amount to be determined by the Court, upon the recommendation of the probation officer.

5. The defendant shall participate the Treasury Offset Program (TOP) as directed by the probation officer.

6. The defendant shall pay the balance owed on any court-ordered financial obligations in installments of not less than $50.00 per month, or 25% of his net monthly income, whichever greater, starting 60 days after supervision begins until paid in full.

7. If the defendant tests positive for a controlled substance or shows signs of alcohol abuse, he shall participate in a program approved by the United States Probation Office for substance abuse, which program may include residential treatment and testing to determine whether the defendant has reverted to the use of drugs or alcohol, with partial costs to be paid by the defendant, all as directed by the probation officer

8. The defendant shall participate in a program approved by the United States Probation Office for mental health treatment, with costs of these programs to be paid by the defendant, all as directed by the probation officer.

9. The defendant shall waive all rights of confidentiality regarding substance abuse and mental health treatment in order to allow for the release of information to the United States Probation Office and authorize communication between the probation officer and the treatment provider(s).

10. The defendant shall participate in a General Educational Development (GED) program approved by the United States Probation Office until he has earned his certificate of completion.

11. The defendant shall participate in vocational, educational, and/or job readiness programs as directed by this Court and identified by the United States Probation Office.

Case Number: 3:19CR00130-001
Defendant's Name: CHATRIE, OKELLO T.

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

	Assessment	Restitution	Fine	AVAA Assessment*	JVTA Assessment**
TOTALS	$ 200.00	$ 196,932.01	$ 0.00	$ 0.00	$ 0.00

☐ The determination of restitution is deferred until _____. An *Amended Judgment in a Criminal Case (AO 245C)* will be entered after such determination.

☒ The defendant must make restitution (including community restitution) to the following payees in the amount listed below.
This amount shall be offset by the money collected at the defendant's house during execution of the search warrant.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all nonfederal victims must be paid before the United States is paid.

Name of Payee	Total Loss***	Restitution Ordered	Priority or Percentage
CALL FEDERAL CREDIT UNION 3640 CALL FEDERAL DRIVE MIDLOTHIAN, VIRGINA 23112		$196,932.01	
TOTAL		**$196,932.01**	

☐ Restitution amount ordered pursuant to plea agreement $

☐ The defendant must pay interest on restitution and a fine of more than $2,500, unless the restitution or fine is paid in full before the fifteenth day after the date of the judgment, pursuant to 18 U.S.C. § 3612(f). All of the payment options on Sheet 6 may be subject to penalties for delinquency and default, pursuant to 18 U.S.C. § 3612(g).

☒ The court determined that the defendant does not have the ability to pay interest and it is ordered that:

☒ the interest requirement is waived for the ☐ fine ☒ restitution.

☐ the interest requirement for the ☐ fine ☐ restitution is modified as follows:

* Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018, Pub. L. No. 115-299.
** Justice for Victims of Trafficking Act of 2015, Pub. L. No. 114-22.
*** Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

Case Number: **3:19CR00130-001**
Defendant's Name: **CHATRIE, OKELLO T.**

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

A ☐ Lump sum payment of $_____ due immediately, balance due
☐ not later than _____ , or
☐ in accordance with ☐ C, ☐ D, ☐ E, or ☐ F below; or

B ☒ Payment to begin immediately (may be combined with ☐ C, ☒ D, or ☐ F below); or

C ☐ Payment in equal *(e.g., weekly, monthly, quarterly)* installments of $ over a period of *(e.g., months or years)*, to commence *(e.g., 30 or 60 days)* after the date of this judgment; or

D ☒ Payment in equal monthly installments of **$50.00,** to commence **60 days** after release from imprisonment to a term of supervision; or

E ☐ Payment during the term of supervised release will commence within *(e.g., 30 or 60 days)* after release from imprisonment. The court will set the payment plan based on an assessment of the defendant's ability to pay at that time; or

F ☐ Special instructions regarding the payment of criminal monetary penalties:

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during the period of imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

☐ Joint and Several

Case Number Defendant and Co-Defendant Names *(including defendant number)*	Total Amount	Joint and Several Amount	Corresponding Payee, if appropriate

☐ The defendant shall pay the cost of prosecution.

☐ The defendant shall pay the following court cost(s):

☒ The defendant shall forfeit the defendant's interest in the following property to the United States:

See *Consent Order of Forfeiture* entered by the Court on May 9, 2022, which is incorporated by reference into this judgment.

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) AVAA assessment, (5) fine principal, (6) fine interest, (7) community restitution, (8) JVTA assessment, (9) penalties, and (10) costs, including cost of prosecution and court costs.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Case No. 3:19cr130**
	)	**The Honorable M. Hannah Lauck**
OKELLO T. CHATRIE,	)	
Defendant	)	

NOTICE OF APPEAL

Okello Chatrie, through counsel, notes his appeal to the United States Court of Appeals for the Fourth Circuit from the final order in this case entered on August 19, 2022 (ECF No. 239).

Respectfully Submitted,
OKELLO T. CHATRIE

By: _____/s/_____
Counsel

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Richmond Division (The Hon. M. Hannah Lauck)

JOINT APPENDIX

VOLUME 7 of 11 (pages 1457 - 1810)

JESSICA D. ABER
United States Attorney

Kenneth R. Simon, Jr., Ass't U.S. Attorney
Peter S. Duffey, Ass't U.S. Attorney
Counsel for Appellee
919 East Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400

Nathan P. Judish, Senior Counsel
Computer Crime & Intel. Property Section
Criminal Division
U.S. Department of Justice

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
Counsel for Appellant
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800

Michael W. Price, Litigation Dir.
NACDL Fourth Amendment Ctr.
1660 L Street NW, 12th Floor
Washington, DC 20036

This page intentionally left blank for double-sided pagination and printing

TABLE OF CONTENTS

VOLUME 1 (pages 1 - 176)

District Court Docket Sheet (as of Jan. 17, 2023) 1

Indictment (Sept. 17, 2019, Doc. 1) 22

Defendant's Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Oct. 29, 2019, Doc. 29) 25

Government's Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (Nov. 19, 2019, Doc. 41) 51

Defendant's Reply to Government's Response [to] Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Dec. 9, 2019, Doc. 48) 76

Exh. A (First Step 2 Request to Google) (Doc. 48-1) 98
Exh. B (Second Step 2 Request to Google) (Doc. 48-2) 100
Exh. C (Third Step 2 Request to Google) (Doc. 48-3) 102
Exh. D (Transcript, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019)) (Doc. 48-4) ..... omitted from J.A.

Government's Notice Regarding Attachment of Google Geofence State Search Warrant to Response in Opposition to Motion to Suppress (Dec. 18, 2019, Doc. 54) 104

Affidavit for search warrant and warrant, with attachments (Doc. 54-1) 107

Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant (Dec. 20, 2019, Doc. 59-1) 118

United States' Response to Amicus Curiae Brief of Google LLC (Jan. 10, 2020, Doc. 71) 148

Defendant's Response to Google's Motion to File Amicus Curiae Brief in Support of Neither Party (Jan. 10, 2020, Doc. 72) 158

VOLUME 2 (pages 177 - 416)

Transcript, Discovery Motion Hearing (Jan. 21, 2020, Doc. 81; *see* Doc. 77 (court minutes))....177

Preliminary matters....179

Def't witness Spencer McInvaille — Direct examination....193; Cross examination....283; Redirect examination....306

Argument by the defense....318
Argument by the government....332
Rebuttal by the defense....350

Court's ruling....355

Defendant's Supplemental Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (May 22, 2020, Doc. 104)....363

United States' Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (June 12, 2020, Doc. 109)....393

VOLUME 3 (pages 417 - 694)

Transcript, Suppression Motion Hearing, Day 1 (evidence) (Mar. 4, 2021, Doc. 201; *see* Doc. 198 (court minutes))....417

Preliminary matters....420

Def't witness Spencer McInvaille — Direct examination....432; Cross examination....542; Redirect examination....586

Def't witness Marlo McGriff — Direct examination....606

VOLUME 4 (pages 695 - 1070)

Transcript, Suppression Motion Hearing, Day 2 (evidence) (Mar. 5, 2021, Doc. 202; *see* Doc. 199 (court minutes)) 695

Preliminary matters 698

Def't witness Marlo McGriff, cont'd — Direct examination ..... 699; Cross examination ..... 791; Redirect examination 841

Def't witness Sarah Rodriguez — Direct examination ..... 862; Cross examination ..... 902; Redirect examination 916

Gov't witness Jeremy D'Errico — Direct examination ..... 923; Cross examination ..... 967; Redirect examination 1010

Gov't witness Joshua Hylton — Direct examination ..... 1016; Cross examination ..... 1040; Redirect examination 1063

Concluding matters 1064

VOLUME 5 (pages 1071 - 1326)

Defendant's Post-Hearing Brief on "Geofence" General Warrant (May 3, 2021, Doc. 205) 1071

Government's Response in Opposition to Defendant's Motion for Suppression (May 21, 2020, Doc. 214; *see* Doc. 207-2) 1117

Defendant's Reply to Government's Response in Opposition to Motion for Suppression (June 4, 2020, Doc. 213) 1164

Transcript, Suppression Hearing (arguments) (June 24, 2021, Doc. 217; *see* Doc. 215 (court minutes)) 1185

Argument by the defense 1187
Argument by the government 1231
Rebuttal by the defense 1313

Concluding matters 1322

VOLUME 6 (pages 1327 - 1456)

Memorandum Opinion (denying suppression motion) (Mar. 3, 2022, Doc. 220) 1327

Order (denying suppression motion) (Mar. 3, 2022, Doc. 221) 1390

Criminal Information (May 6, 2022, Doc. 224) 1391

Transcript, Change of Plea Hearing (May 9, 2022, Doc. 247; *see* Doc. 226) 1394

Plea Agreement (May 9, 2022, Doc. 228) 1428

Statement of Facts (May 9, 2022, Doc. 229) 1444

Judgment in a Criminal Case (Aug. 19, 2022, Doc. 239) 1449

Notice of Appeal (Aug. 25, 2022, Doc. 241) 1456

VOLUME 7 (pages 1457 - 1810) – DOCUMENT EXHIBITS

Exhibits Admitted at Discovery Motion Hearing (Jan. 21, 2020)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) ..... *see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) ..... *see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) ..... *see* J.A. 2093
Def't Exh. 4: Activation Video ..... omitted from J.A., available on request
Def't Exh. 5: Three Paths Video (sealed) ..... *see* J.A. 2139
Def't Exh. 6: First Step 2 Request to Google 1457
Def't Exh. 7: Second Step 2 Request to Google 1459
Def't Exh. 8: Third Step 2 Request to Google 1461

Def't Exh. 9: Step 3 Request to Google 1463

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) .....*see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) .....*see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) .....*see* J.A. 2093
Def't Exh. 5: Three Paths Video (sealed) .....*see* J.A. 2139
Def't Exh. 6: Spencer McInvaille Report 1464
Def't Exh. 7: Spencer McInvaille Supplemental Report 1469
Def't Exh. 8: CSV Google Data File (.csv file) .....*see* J.A. 2139
Def't Exh. 9: Unique in Crowd Study 1475
Def't Exh. 11: September 2018 Oracle Submission 1480
Def't Exh. 18: Federal Search Warrant Application & Attachments 1502
Def't Exh. 19: State Search Warrants & Attachments 1534
Def't Exh. 21: McGriff Declaration 1 (Doc. 96-1) 1551
Def't Exh. 23: McGriff Declaration 3 (Doc. 147) 1562
Def't Exh. 24: Rodriguez Declaration (Doc. 96-2) 1579
Def't Exh. 27: Every Step You Take 1587
Def't Exh. 30: AZ Ex. 18 (admitted portions only) 1631
Def't Exh. 31: AZ Ex. 19 (admitted portions only) 1633
Def't Exh. 32: AZ Ex. 20 1639
Def't Exh. 33: AZ Ex. 24 1644
Def't Exh. 34: AZ Ex. 202 1667
Def't Exh. 36: AZ Ex. 209 1777
Def't Exh. 38: AZ Ex. 219 1781
Def't Exh. 40: AZ Ex. 236 1797
Def't Exh. 41: AZ Ex. 260 1804

VOLUME 8 (pages 1811 - 2090) – DOCUMENT EXHIBITS, CONT'D

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021), cont'd

Def't Exh. 43: May 2018 Privacy Policy – Redline 1811
Def't Exh. 43a: May 2018 Privacy Policy – Redline (with internet source information) 1840
Def't Exh. 44: Jan. 2019 Privacy Policy – Redline 1865
Def't Exh. 45: Oct. 2019 Privacy Policy – Redline 1895
Def't Exh. 46: McGriff Blog 1 1926

Def't Exh. 47: McGriff Blog 2 1929
Def't Exh. 48: 2018 Quartz Article 1934
Def't Exh. 49: 2018 AP Article 1 1941
Def't Exh. 51: 2019 NYT Article 1948
Def't Exh. 53: Blumenthal-Markey Letter to FTC 1957

Gov't Exh. 1: CAST PowerPoint Presentation 1981
Gov't Exh. 2: Geofence Warrant (Doc. 54-1) ..... *see* J.A. 107
Gov't Exh. 3: Declaration of Marlo McGriff (Mar. 11, 2020)
(same as Def't Exh. 21 (Doc. 96-1)) ..... *see* J.A. 1551
Gov't Exh. 3a: Declaration of Sarah Rodriguez (Mar. 11, 2020)
(same as Def't Exh. 24 (Doc. 96-2)) ..... *see* J.A. 1579
Gov't Exh. 3b: Supplemental Declaration of McGriff (June 17, 2020)
(Doc. 110-1) 2032
Gov't Exh. 3c: Third Declaration of Marlo McGriff (Aug. 7, 2020)
(same as Def't Exh. 23 (Doc. 147)) ..... *see* J.A. 1562
Gov't Exh. 4: Joshua Hylton emails with Google 2034
Gov't Exh. 5: Google Privacy Policy 2048
Gov't Exh. 5a: Google Terms of Service 2081
Gov't Exh. 6: Special Agent D'Errico's C.V. 2088
Gov't Exh. 12: "Got to Be Mobile" Video ..... *see* J.A. 2091

VOLUME 9 (pages 2091 - 2092) – DIGITAL MEDIA EXHIBIT

Gov't Exh. 12: "Got to Be Mobile" Video (admitted only at suppression motion hearing) ..... (.mp4 file)

VOLUME 10 (pages 2093 - 2138) – SEALED DOCUMENT EXHIBIT

Def't Exh. 3: PDF of Raw Data (*see* Doc. 69 (sealing order)) (admitted at both discovery motion hearing and suppression motion hearing) 2093

VOLUME 11 (pages 2139 - end) – SEALED DIGITAL MEDIA EXHIBITS

Def't Exh. 5: Three Paths Video (admitted at both discovery motion hearing and suppression motion hearing) ..... (.mp4 file)
Def't Exh. 8: CSV Google Data File (admitted only at suppression motion hearing) ..... (.csv file, viewable in Excel)

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472
Importance: High

Google Legal Team,

I'm writing to inquire about my correspondence with your office on 07/01 and 07/02. Please keep in mind that expedition is requested based on armed and dangerous subject(s) still being at large. Subject was on cell phone just prior to violent act; therefore, Google may have captured pertinent information to identify and arrest parties involved. See below:

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

As discussed yesterday over the phone, I appreciate your quick response and willingness to provide GPS data for the below device ID(s). Please expedite this request where possible due to this suspect's continued threat to our community. If it would speed up the process, please provide data as it becomes accessible/available, starting with device ID(s) 1 – 9. It was mentioned that the larger the request, the more time it will take to get data back. With this in mind, I will still have to rule out device ID(s) 1-9; however, I may be able to do so more quickly if I can begin reviewing data. The faster I can review the data, the faster I can get this guy/guys off the street.

Thanks again for your professionalism and understanding. I realize that I'm asking for a lot and you and your team are likely tasked-out already, but any and all assistance and expedited process is MUCH appreciated.

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

Thank you guys for the extremely quick turnaround on the Stage Two data. After plotting the nine device ID(s) with additional geographical data, I have narrowed my search for subscriber info to three device ID(s):

1. **1716665659**
2. 907512662
3. -1662304683

Please send me the subscriber information for the above device ID(s) as soon as possible. The involved offender is still a threat to the community and may be a flight risk as well. Again, I can't thank the Google Legal team enough for your professionalism, quick response, and understanding in the captioned matter.

If you have any questions or concerns, please don't hesitate to call, [redacted].

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."



Report Prepared for:

United States vs. Okello Chatrie

Spencer J. McInvaille CTNS, CWA, CCO, CCPA
Digital Forensic Examiner and Cellular Analyst
2700 Gateway Centre Blvd, Suite 100
Morrisville, NC 27560

Case Analysis:

I am aware that, according to Google, Location History (LH) was enabled July 9, 2018, at approximately 04:09 (UTC) (July 9, 2018, 00:09 Eastern) for the account related to this case (okellochatrie55@gmail.com). I was asked to determine what occurred on the device in close proximity to that date and time and identify any actions that could have resulted in enabling location history.

I met with Agent D'Errico at the Richmond FBI Office on October 14, 2020, to conduct a new examination of the Samsung S9+ (SM-G965U) device related to this case. The first examination was completed by the FBI using Cellebrite forensic software, specifically "Advanced logical" method. Since that examination, Cellebrite has updated its software to allow for a much more in-depth look into the data stored on the device. Specifically, Cellebrite's update provided two new methods of extraction types: Qualcomm Live Physical and Qualcomm Live Full File System. The Physical and File System extraction allows an examiner to review the databases in the device for critical file system information in addition to, data that had not been previously obtained from the previous advanced logical extraction. I conducted three new extractions, one with each of the available methods: Qualcomm Live Physical, Qualcomm Live Full File System and Advanced Logical.

A Physical extraction is a bit for bit copy of the flash memory of the device and stores that data within a binary file. These files can be analyzed using forensic software such as Cellebrite Physical Analyzer. This is the most comprehensive extraction method available.

A Full File System extraction extracts all files present in the internal memory, including database files, system files, and logs. It allows for the examiner to see file structure, web browsing history, and app usage history of a mobile device, etc., via the data from the database files obtained.

The Advanced Logical Extraction methods gather data from the device using requests and is a combined file system and logical extraction.

I took the following steps in conducting the three extractions on the Samsung S9+ device: While onsite, I was provided the Samsung S9+ device held in evidence by the FBI. Once removed from the evidence bag, the phone was moved to a faraday bag for startup. This ensures that the device is unable to send or receive information to the cellular or other networks. Once powered on, I checked to ensure that airplane mode was enabled, and it was enabled at startup. I removed the device from the faraday bag to begin the extraction processes.

I was also provided with the swipe pattern needed for unlocking the device. Using Cellebrite Universal Forensic Extraction Device and running software version 7.38.0.12 (the most current version available on this date), I researched the device and I determined that the device was compatible with the Qualcomm Live Physical Extraction method. Following the on-screen steps provided by Cellebrite, I enabled developer options, USB debugging, and stay awake on the device, turned off the lock screen security, and proceeded with the extraction.

Once the Physical extraction was successfully completed, I repeated the process to conduct the Full File System extraction. Once successfully completed, I moved on to conduct the Advanced Logical extraction method. This extraction method was also completed. All extractions were written to an external storage source, and a copy was also provided to Agent D'Errico.

Following the onsite extractions, I have analyzed the data offsite as follows; Using the Cellebrite Physical Analyzer (PA) software, I began to review the data extracted from the device. The size of the data for all three extractions is approximately 85 gigabytes. I used Physical Analyzer to verify the integrity of the extractions, which verified the reference hash values were correct.

The process of reviewing extracted cell phone data contained can be simple or complex. The Physical Analyzer "parses" data into information easily understood and commonly provided in courtrooms. For example, text messages and calls are often shown in court in tables or conversations that clearly show the content of the communications. However, the Physical Analyzer does not parse all data contained within the extractions. Some portions of the data require manual examination. A manual exam requires an examiner to individually look through each file path in the file system and review each of the databases contained within them. Databases consist of tables of data, which can be analyzed within Physical Analyzer or other commercially available forensic software suites.

The review of this information takes a considerable amount of time for at least two reasons. First, the analysis of data bases requires following each path and opening the databases and their associated content to locate information you are looking for. Second, times and other information in these tables often require one to convert them into information that can be understood. Times in these tables are often stored in milliseconds from UTC 1970 (Unix time). At the time of this report, I am still in review of the databases contained within the data obtained from the extractions.

Once the data was loaded in Physical Analyzer, I began my analysis of the data. In Physical Analyzer, I searched for any application usage or other data that occurred within close proximity to July 9, 2018, at approximately 04:09 (UTC) (July 9, 2018, 00:09 Eastern).

Within “Installed Applications” parsed by Physical Analyzer, I noted several applications with timestamps on the date July 9, 2018. “Installed Applications” is the naming convention within the Cellebrite software for parsed data related to application installs and updates. The Cellebrite software parses this information from the localppstate.db (database). The localappstate.db contains information regarding the installation/updates of applications and the account associated with the install. This information was located within the following path; userdata(ExtX)/Root/data/com.android.vending/databases/localappstate.db.

The applications associated with the okellochatrie55@gmail.com account listed during this timeframe were; Google Quick Search box, Amazon Prime Video, Google Assistant, Samsung Calculator, Samsung Device Care, Flipboard, and Samsung Always on Display. Only two of these applications are Google applications: Google Quick Search Box and Google Assistant.

Google Quick Search Box indicates a timestamp in the database of July 9, 2018 19:58:54 UTC, over 13 hours after Google reported that Google Location History was enabled. Google Assistant, however, shows “single_install” on the date of July 9, 2018, 04:06:51 UTC. This installation of Google Assistant occurs very close to the time noted by Google, “July 9, 2018, at approximately 04:09 (UTC)” (July 9, 2018, 00:09 Eastern) and the times indicated in the Audit report listed below that Google provided.

The Audit Report provided by Google indicates changes made to the Google Location History setting for the okellochatrie55@gmail.com account. The Audit Report indicates three timestamps (conversion shown for Milliseconds from UTC 1970):

Server_creation_time_millis: 1531109348611 (Jul 09 2018 04:09:08 UTC)

Client_creation_time_millis: 1531109245034 (Jul 09 2018 04:07:25 UTC)

Client_upload_time_millis: 1531109347486 (Jul 09 2018 04:09:07 UTC)

Google has confirmed that Location History was enabled by a device-based opt-in. Google has further indicated there are only two ways a device-based opt-in can occur: (1) directly through the device settings application or (2) through the “consent flow” (pop up box) on a supported Google Application. Google also indicates the consent flow can be prompted when attempting to use a feature supported by Location History. Google Assistant is an application supported by Location History.

It is my opinion based on the information from Google and the data located during the search of the device, that it is likely Google Location History was enabled using the Google Assistant application. As of the date of this report, I have located no other applications that would be consistent with the enabling of Google Location History.

End of Report



Report Prepared for:

United States vs. Okello Chatrie

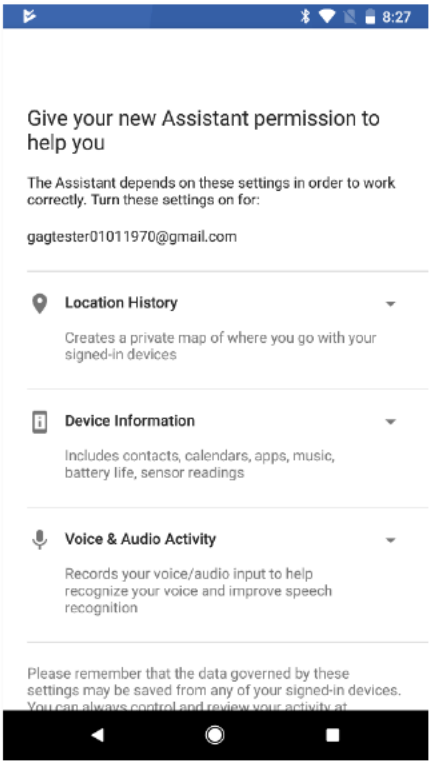
Spencer J. McInvaille CTNS, CWA
Digital Forensic Examiner and Cellular Analyst
2700 Gateway Centre Blvd, Suite 100
Morrisville, NC 27560

Google indicates it has no documentation of the process or application used to enable Location History for the okellochatrie55@gmailcom account. Due to the lack of specific details documenting Location History's activation on Mr. Chatrie's phone, I analyzed the possible ways that Location History could have been activated. As further detailed in my initial report, that analysis indicated Google Assistant likely enabled Location History. That analysis revealed the installation of Google Assistant moments before activation of Location History. This report documents publicly available information and defense investigation regarding the setup and methods to enable Location History upon first use of Google Assistant.

In conducting this analysis, I reviewed the publicly available information regarding the Location History opt-in process related to Google Assistant. Google describes Google Assistant as a productivity application that allows you to get hands-free help, get quick directions, search the internet, set helpful reminders, and other user convenience tasks. Internet searches and further investigation yielded examples of the opt-in methods, specifically when using Google Assistant. Examples contemporaneous to this case appear to be the most reliable way to document the opt-in process. Due to the updates to software and Googles' policies since Location History's activation on the oklellochatrie55@gmail.com account, I cannot replicate the opt-in process Mr. Chatrie would have seen. The examples below should provide the clearest picture of the opt-in process using Google Assistant that he would have seen.

On an Android device with Google Assistant, the user may launch the Google Assistant application by long-pressing the home button. Upon first use, the application will prompt the user to allow permissions. These permissions include Location History. Mr. McGriff describes a version of this permission screen in his third declaration. He omits, however, that the permission screen requested two other permissions, not just Location History.

Figure 1: Quartz Screenshot



I located several sources that document the process for enabling Location History and specifically enabling location history through Google Assistant. The first is from Quartz (qz.com). Quartz published an article on January 24, 2018, discussing the opt-in process for Location History. (https://qz.com/1183559/if-youre-using-an-android-phone-google-may-be-tracking-every-move-you-make/). The author, David Yanofsky, provides a description and screen captures of these processes. Counsel for Mr. Chatrie contacted Mr. Yanofsky to obtain the actual screen capture from the article, shown in Figure 1, taken on January 18, 2018. Mr. Yanofsky further confirmed that he took this screen capture using a Google Pixel 2 phone, running Android 8.1.

Mr. Yanofsky specifically addresses the opt-in process for Location History through Google Assistant. Mr. Yanofsky describes, upon first use, Google Assistant prompts the user to enable Location History. The article does not provide any other information about the expansion arrows menus you see on the screen.

Oracle, a computer technology company, completed a study in 2018 which details Google's collection of user data. Oracle documented Google's steps for the activation of Location History through several methods, including Google Assistant. In the document labeled "Google, Android and Location Tracking" from September 2018, Oracle discusses location history and other Google services. On page 4, Oracle displays the setup screen for Google Assistant. Oracle also displays the screen once you select "Next." The subsequent screen capture is the same as Quartz, but the selections for "No Thanks" and "Yes I'm In" are visible. Shown in Figure 2 is a screen capture from Oracles' document.

Figure 2: Oracle Screen Capture

Continuing through the Android smartphone setup process, users are prompted to enable **Google Assistant**[6] – a step that enables Location History, collection of device information, and recording of voice and audio activity of the user. Figure 3 displays the screenshots for setup of the Google Assistant service, bundling multiple settings with one "Yes I'm In". These default settings for Google Assistant also meet the criteria for an "opt-out" process, in direct conflict with Google's statement that "users must opt-in to this service."[7]

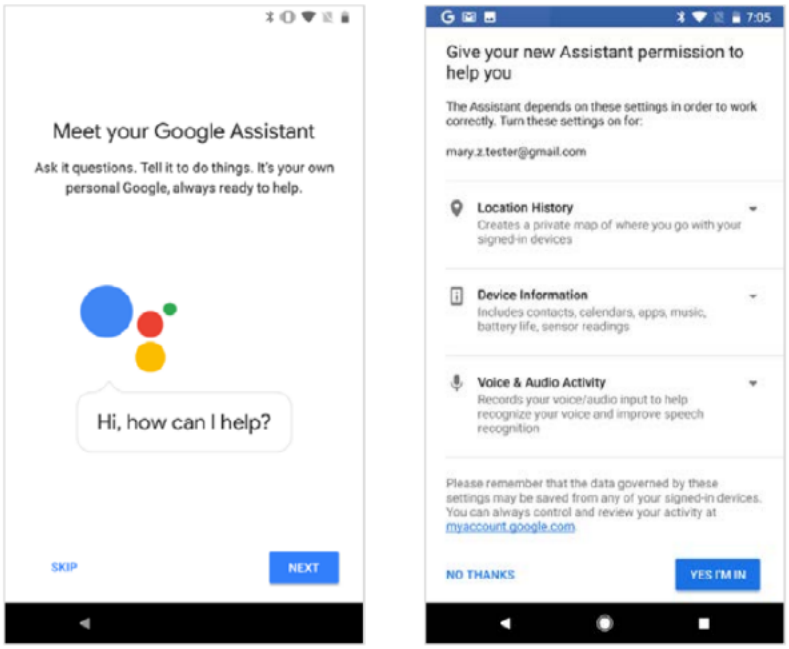


Figure 3: Google Assistant Setup Screens

https://www.accc.gov.au/system/files/Oracle-Submission-2-%28September-2018%29.pdf

I also reviewed screen captures from a report completed by Forbrukerradet (Norwegian Consumer Council), "Every Step You Take." Screen captures were made during the setup of a Samsung Galaxy S7. The device setup occurred on July 2, 2018, on Android version 8.0. A device setup was also completed using the same device on August 9, 2018. All screen captures from both dates produced were provided to counsel for Mr. Chatrie from Forbrukerradet. The screen captures are from a factory reset device and details each screen the user sees through the process and any expansion arrows menus and selections.

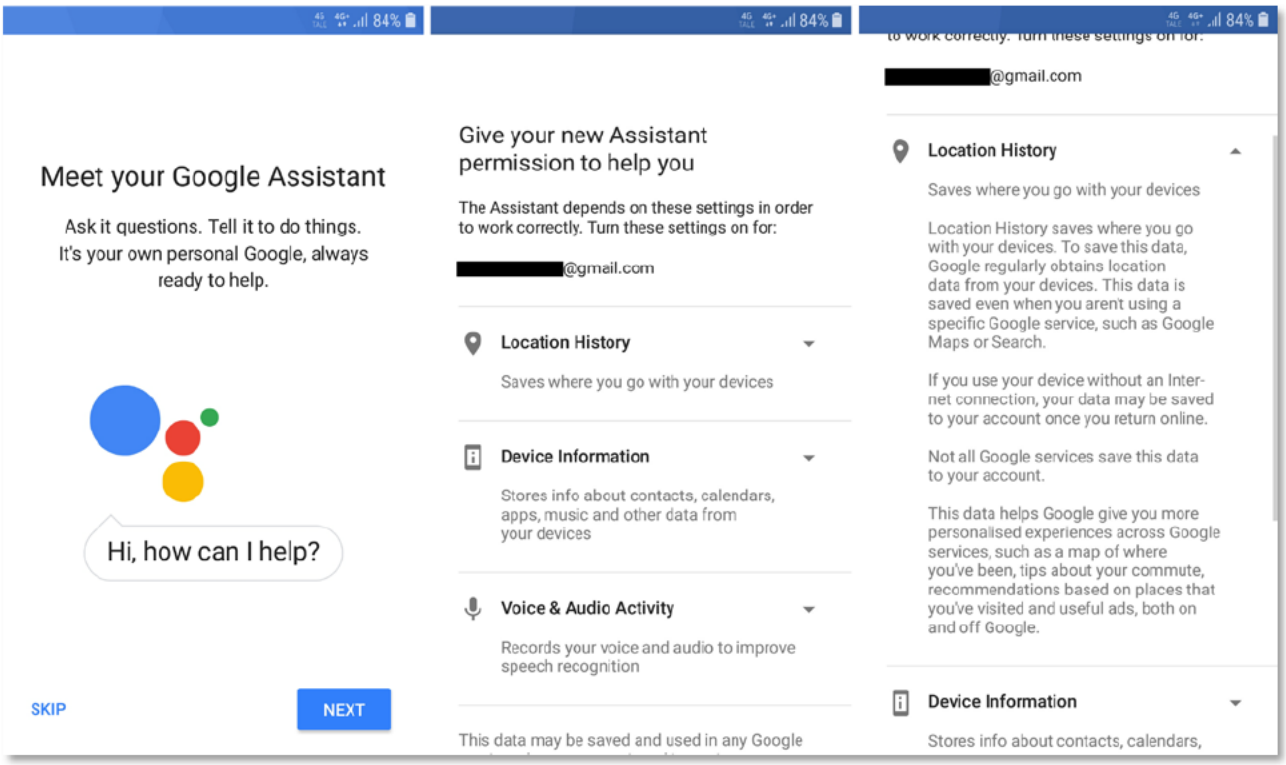
The Google Assistant setup begins with the "Meet Google Assistant" screen, with "Skip" and "Next" choices. Selecting "Next" prompts a permissions screen. Google displays, "The Assistant depends on

these settings in order to work correctly." "No, thanks" and "Turn On" are choices for the permissions screen.

In the previous captures for the permissions screen, the expansion arrows and their contents were unavailable. The opening of each expansion arrow is not required to make a selection at the bottom of the screen, meaning a user can activate Google Assistant without looking at the expansion arrows. The screen captures from the July 2, 2018 test show each of the expansion arrows. Expansion arrows for Location History, Device Information, and Voice & Audio Activity are displayed. I note the description under the Location History permission changed at some point between the previous examples. The description changes from "Creates a private map of where you go with your signed-in devices" to "Saves where you go with your devices." Google, in Marlo McGriff's third affidavit, indicates that "Saves Where you go with your device" was the wording used during the time of this case. The screen captures referenced are shown below.

(https://fil.forbrukerradet.no/wpcontent/uploads/2018/11/27-11-18-every-step-you-take.pdf)

Figure 3: Norwegian Consumer Council Screenshots 7/2/2018



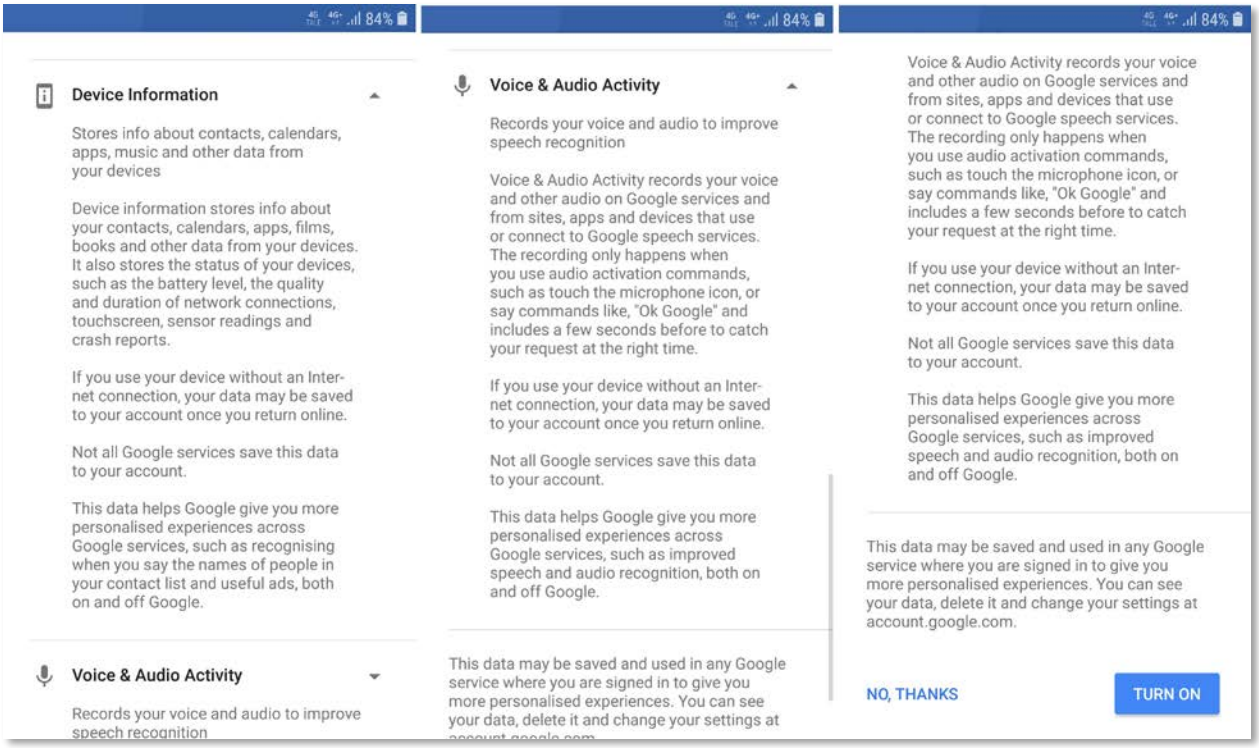
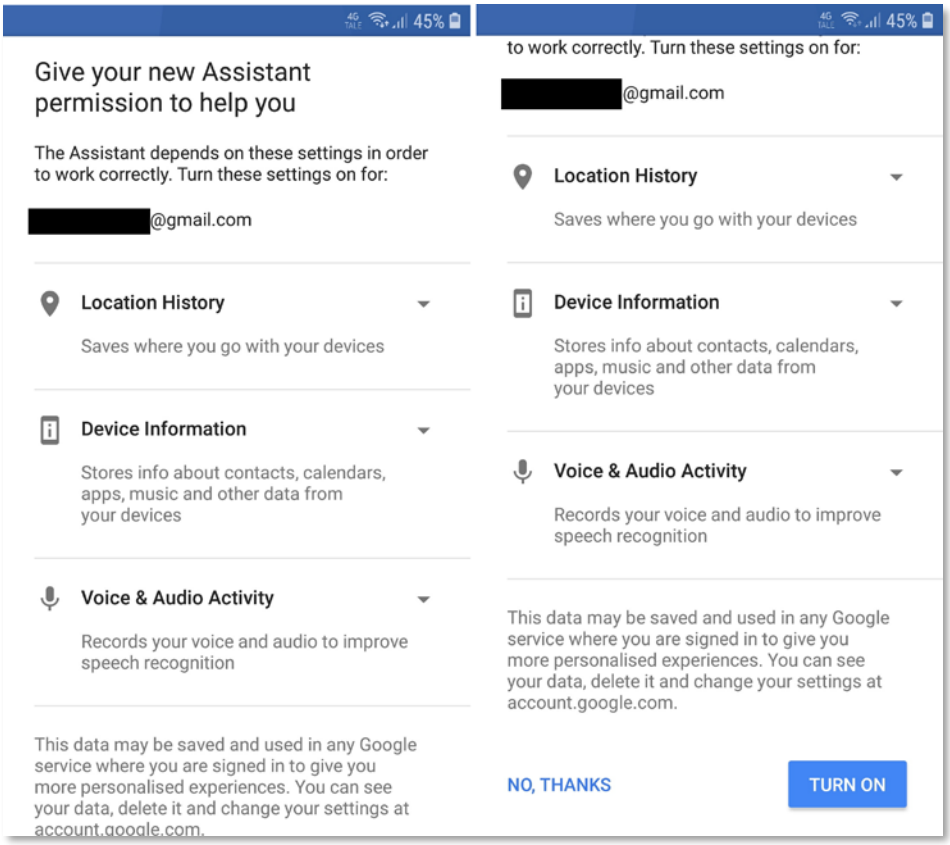


Figure 4: Norwegian Consumer Council Screenshots 8/9/2018



The examples in each of the documents show consistent screens and selections for enabling Location History through the Google Assistant application. By selecting "Turn On," the user enables Location History, and the account begins to collect and store location data immediately from reporting devices. The user does not need to actually use Google Assistant after installation to generate location data stored within the account. If the device is powered on, it will passively collect and report location data. By choosing to enable Location History, the user will now create location data within the account for the device's life. Deleting the application used to enable Location History does not stop the collection and storage of location data.

End of Report

SCIENTIFIC REPORTS



OPEN

SUBJECT AREAS:
APPLIED PHYSICS
APPLIED MATHEMATICS
STATISTICS
COMPUTATIONAL SCIENCE

Received
1 October 2012

Accepted
4 February 2013

Published
25 March 2013

Correspondence and requests for materials should be addressed to Y.-A. de M. (yva@mit.edu)

Unique in the Crowd: The privacy bounds of human mobility

Yves-Alexandre de Montjoye[1,2], César A. Hidalgo[1,3,4], Michel Verleysen[2] & Vincent D. Blondel[2,5]

[1]Massachusetts Institute of Technology, Media Lab, 20 Ames Street, Cambridge, MA 02139 USA, [2]Université catholique de Louvain, Institute for Information and Communication Technologies, Electronics and Applied Mathematics, Avenue Georges Lemaître 4, B-1348 Louvain-la-Neuve, Belgium, [3]Harvard University, Center for International Development, 79 JFK Street, Cambridge, MA 02138, USA, [4]Instituto de Sistemas Complejos de Valparaíso, Paseo 21 de Mayo, Valparaíso, Chile, [5]Massachusetts Institute of Technology, Laboratory for Information and Decision Systems, 77 Massachusetts Avenue, Cambridge, MA 02139, USA.

We study fifteen months of human mobility data for one and a half million individuals and find that human mobility traces are highly unique. In fact, in a dataset where the location of an individual is specified hourly, and with a spatial resolution equal to that given by the carrier's antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals. We coarsen the data spatially and temporally to find a formula for the uniqueness of human mobility traces given their resolution and the available outside information. This formula shows that the uniqueness of mobility traces decays approximately as the 1/10 power of their resolution. Hence, even coarse datasets provide little anonymity. These findings represent fundamental constraints to an individual's privacy and have important implications for the design of frameworks and institutions dedicated to protect the privacy of individuals.

Derived from the Latin Privatus, meaning "withdraw from public life," the notion of privacy has been foundational to the development of our diverse societies, forming the basis for individuals' rights such as free speech and religious freedom[1]. Despite its importance, privacy has mainly relied on informal protection mechanisms. For instance, tracking individuals' movements has been historically difficult, making them de-facto private. For centuries, information technologies have challenged these informal protection mechanisms. In 1086, William I of England commissioned the creation of the Doomsday book, a written record of major property holdings in England containing individual information collected for tax and draft purposes[2]. In the late 19th century, de-facto privacy was similarly threatened by photographs and yellow journalism. This resulted in one of the first publications advocating privacy in the U.S. in which Samuel Warren and Louis Brandeis argued that privacy law must evolve in response to technological changes[3].

Modern information technologies such as the Internet and mobile phones, however, magnify the uniqueness of individuals, further enhancing the traditional challenges to privacy. Mobility data is among the most sensitive data currently being collected. Mobility data contains the approximate whereabouts of individuals and can be used to reconstruct individuals' movements across space and time. Individual mobility traces T [Fig. 1A–B] have been used in the past for research purposes[4–18] and to provide personalized services to users[19]. A list of potentially sensitive professional and personal information that could be inferred about an individual knowing only his mobility trace was published recently by the Electronic Frontier Foundation[20]. These include the movements of a competitor sales force, attendance of a particular church or an individual's presence in a motel or at an abortion clinic.

While in the past, mobility traces were only available to mobile phone carriers, the advent of smartphones and other means of data collection has made these broadly available. For example, Apple® recently updated its privacy policy to allow sharing the spatio-temporal location of their users with "partners and licensees"[21]. 65.5B geo-tagged payments are made per year in the US[22] while Skyhook wireless is resolving 400 M user's WiFi location every day[23]. Furthermore, it is estimated that a third of the 25B copies of applications available on Apple's App Store℠ access a user's geographic location[24,25], and that the geo-location of ~50% of all iOS and Android traffic is available to ad networks[26]. All these are fuelling the ubiquity of simply anonymized mobility datasets and are giving room to privacy concerns.

A simply anonymized dataset does not contain name, home address, phone number or other obvious identifier. Yet, if individual's patterns are unique enough, outside information can be used to link the data back to an individual. For instance, in one study, a medical database was successfully combined with a voters list to extract

www.nature.com/scientificreports

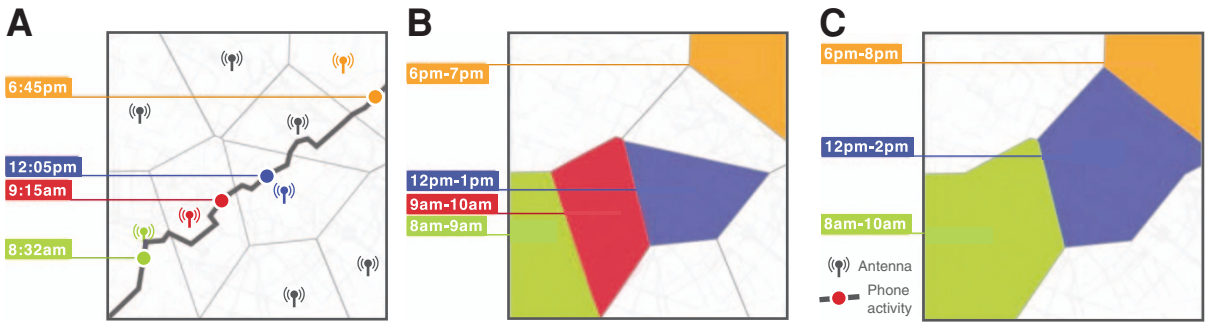


Figure 1 | (A) Trace of an anonymized mobile phone user during a day. The dots represent the times and locations where the user made or received a call. Every time the user has such an interaction, the closest antenna that routes the call is recorded. (B) The same user's trace as recorded in a mobility database. The Voronoi lattice, represented by the grey lines, are an approximation of the antennas reception areas, the most precise location information available to us. The user's interaction times are here recorded with a precision of one hour. (C) The same individual's trace when we lower the resolution of our dataset through spatial and temporal aggregation. Antennas are aggregated in clusters of size two and their associated regions are merged. The user's interaction are recorded with a precision of two hours. Such spatial and temporal aggregation render the 8:32 am and 9:15 am interactions indistinguishable.

the health record of the governor of Massachusetts[27]. In another, mobile phone data have been re-identified using users' top locations[28]. Finally, part of the Netflix challenge dataset was re-identified using outside information from The Internet Movie Database[29].

All together, the ubiquity of mobility datasets, the uniqueness of human traces, and the information that can be inferred from them highlight the importance of understanding the privacy bounds of human mobility. We show that the uniqueness of human mobility traces is high and that mobility datasets are likely to be re-identifiable using information only on a few outside locations. Finally, we show that one formula determines the uniqueness of mobility traces providing mathematical bounds to the privacy of mobility data. The uniqueness of traces is found to decrease according to a power function with an exponent that scales linearly with the number of known spatio-temporal points. This implies that even coarse datasets provide little anonymity.

Results

Uniqueness of human mobility. In 1930, Edmond Locard showed that 12 points are needed to uniquely identify a fingerprint[30]. Our unicity test estimates the number of points p needed to uniquely identify the mobility trace of an individual. The fewer points needed, the more unique the traces are and the easier they would be to re-identify using outside information. For re-identification purposes, outside observations could come from any publicly available information, such as an individual's home address, workplace address, or geo-localized tweets or pictures. To the best of our knowledge, this is the first quantification of the uniqueness of human mobility traces with random points in a sparse, simply anonymized mobility dataset of the scale of a small country.

Given I_p, a set of spatio-temporal points, and D, a simply anonymized mobility dataset, we evaluate ε, the uniqueness of traces, by extracting from D the subset of trajectories $S(I_p)$ that match the p points composing I_p [See Methods]. A trace is unique if $|S(I_p)| = 1$, containing only one trace. For example, in Fig. 2A, we evaluate the uniqueness of traces given $I_{p=2}$. The two spatio-temporal points contained in $I_{p=2}$ are zone I from 9am to 10am and zone II from 12pm to 1pm. The red and the green traces both satisfy $I_{p=2}$, making them not unique. However, we can also evaluate the uniqueness of traces knowing $I_{p=3}$, adding as a third point zone III between 3pm and 4pm. In this case $|S(I_{p=3})| = 1$, uniquely characterize the green trace. A lower bound on the risk of deductive disclosure of a user's identity is given by the uniqueness of his mobility trace, the likelihood of this brute force characterization to succeed.

Our dataset contains 15 months of mobility data for 1.5 M people, a significant and representative part of the population of a small European country, and roughly the same number of users as the location-based service Foursquare®[31]. Just as with smartphone applications or electronic payments, the mobile phone operator records the interactions of the user with his phone. This creates a comparable longitudinally sparse and discrete database [Fig. 3]. On average, 114 interactions per user per month for the nearly 6500 antennas are recorded. Antennas in our database are distributed throughout the country and serve, on average, $\sim$ 2000 inhabitants each, covering areas ranging from 0.15 km^2 in cities to 15 km^2 in rural areas. The number of antennas is strongly correlated with population density ($R^2 = .6426$) [Fig. 3C]. The same is expected from businesses, places in location-based social networks, or WiFi hotspots.

Fig. 2B shows the fraction of unique traces (ε) as a function of the number of available points p. Four randomly chosen points are enough to uniquely characterize 95% of the users ($\varepsilon > .95$), whereas two randomly chosen points still uniquely characterize more than 50% of the users ($\varepsilon > .5$). This shows that mobility traces are highly unique, and can therefore be re-identified using little outside information.

Scaling properties. Nonetheless, ε depends on the spatial and temporal resolution of the dataset. Here, we determine this dependence by lowering the resolution of our dataset through spatial and temporal aggregation [Fig. 1C]. We do this by increasing the size of a region, aggregating neighbouring cells into clusters of ν cells, or by reducing the dataset's temporal resolution, increasing the length of the observation time window to h hours [see Methods]. Both of these aggregations are bound to decrease ε, and therefore, make re-identification harder.

Fig. 4A shows how the uniqueness of mobility traces ε depends on the spatial and temporal resolution of the data. This reduction, however, is quite gradual. Given four points (p=4), we find that $\varepsilon > .5$ when using a resolution of $h = 5$ hours and $\nu = 5$ antennas.

Statistically, we find that traces are more unique when coarse on one dimension and fine along another than when they are medium-grained along both dimensions. Indeed, given four points, $\varepsilon > .6$ in a dataset with a temporal resolution of $h = 15$ hours or a spatial resolution of $\nu = 15$ antennas while $\varepsilon > .4$ in a dataset with a temporal resolution of $h = 7$ hours and a spatial resolution of $\nu = 7$ antennas [Fig. 4A].

Next, we show that it is possible to find one formula to estimate the uniqueness of traces given both, the spatial and temporal resolution of the data, and the number of points available to an outside observer. Fig. 4B and 4C show that the uniqueness of a trace decreases as the power function $\varepsilon = \alpha - x^{\beta}$, for decreases in both the spatial and temporal resolution (x), and for all considered $p = 4, 6, 8$ and 10 (see Table S1). The uniqueness of human mobility can thus be expressed using the single formula: $\varepsilon = \alpha - (\nu h)^{\beta}$. We find that this power

www.nature.com/scientificreports

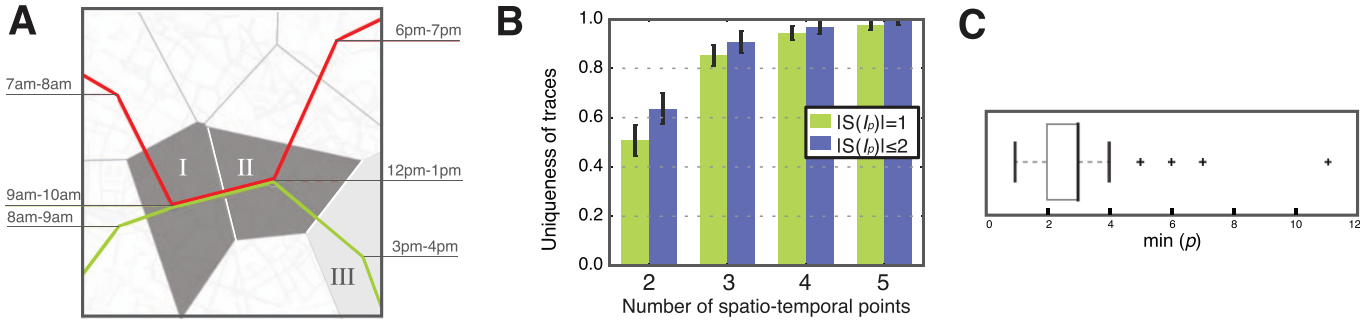


Figure 2 | (A) $I_{p=2}$ means that the information available to the attacker consist of two 7am-8am spatio-temporal points (I and II). In this case, the target was in zone I between 9am to 10am and in zone II between 12pm to 1pm. In this example, the traces of two anonymized users (red and green) are compatible with the constraints defined by $I_{p=2}$. The subset $S(I_{p=2})$ contains more than one trace and is therefore not unique. However, the green trace would be uniquely characterized if a third point, zone III between 3pm and 4pm, is added ($I_{p=3}$). (B) The uniqueness of traces with respect to the number p of given spatio-temporal points (I_p). The green bars represent the fraction of unique traces, i.e. $|S(I_p)| = 1$. The blue bars represent the fraction of $|S(I_p)| \leq 2$. Therefore knowing as few as four spatio-temporal points taken at random ($I_{p=4}$) is enough to uniquely characterize 95% of the traces amongst 1.5 M users. (C) Box-plot of the minimum number of spatio-temporal points needed to uniquely characterize every trace on the non-aggregated database. At most eleven points are enough to uniquely characterize all considered traces.

function fits the data better than other two-parameters functions such as $\alpha - \exp(\lambda x)$, a stretched exponential $\alpha - \exp x^{\beta}$, or a standard linear function $\alpha - \beta x$ (see Table S1). Both estimators for α and β are highly significant ($p < 0.001$)[32], and the mean pseudo-R^2 is 0.98 for the $I_{p=4}$ case and the $I_{p=10}$ case. The fit is good at all levels of spatial and temporal aggregation [Fig. S3A–B].

The power-law dependency of ε means that, on average, each time the spatial or temporal resolution of the traces is divided by two, their uniqueness decreases by a constant factor $\sim (2)^{-\beta}$. This implies that privacy is increasingly hard to gain by lowering the resolution of a dataset.

Fig. 2B shows that, as expected, ε increases with p. The mitigating effect of p on ε is mediated by the exponent β which decays linearly with p: $\beta = 0.157 - 0.007p$ [Fig. 4E]. The dependence of β on p implies that a few additional points might be all that is needed to identify an individual in a dataset with a lower resolution. In fact, given four points, a two-fold decrease in spatial or temporal resolution makes it 9.3% less likely to identify an individual, while given ten points, the same two-fold decrease results in a reduction of only 6.2% (see Table S1).

Because of the functional dependency of ε on p through the exponent β, mobility datasets are likely to be re-identifiable using information on only a few outside locations.

Discussion

Our ability to generalize these results to other mobility datasets depends on the sensitivity of our analysis to extensions of the data to larger populations, or geographies. An increase in population density will tend to decrease ε. Yet, it will also be accompanied by an increase in the number of antennas, businesses or WiFi hotspots used for localizations. These effects run opposite to each other, and therefore, suggest that our results should generalize to higher population densities.

Extensions of the geographical range of observation are also unlikely to affect the results as human mobility is known to be highly circumscribed. In fact, 94% of the individuals move within an average radius of less than 100 km[17]. This implies that geographical extensions of the dataset will stay locally equivalent to our observations, making the results robust to changes in geographical range.

From an inference perspective, it is worth noticing that the spatio-temporal points do not equally increase the likelihood of uniquely identifying a trace. Furthermore, the information added by a point is highly dependent from the points already known. The amount of information gained by knowing one more point can be defined as the reduction of the cardinality of $S(I_p)$ associated with this extra point. The larger the decrease, the more useful the piece of information is. Intuitively, a point on the MIT campus at 3AM is more likely to make a trace unique than a point in downtown Boston on a Friday evening.

This study is likely to underestimate ε, and therefore the ease of re-identification, as the spatio-temporal points are drawn at random from users' mobility traces. Our I_p are thus subject to the user's spatial and temporal distributions. Spatially, it has been shown that the uncertainty of a typical user's whereabouts measured by its

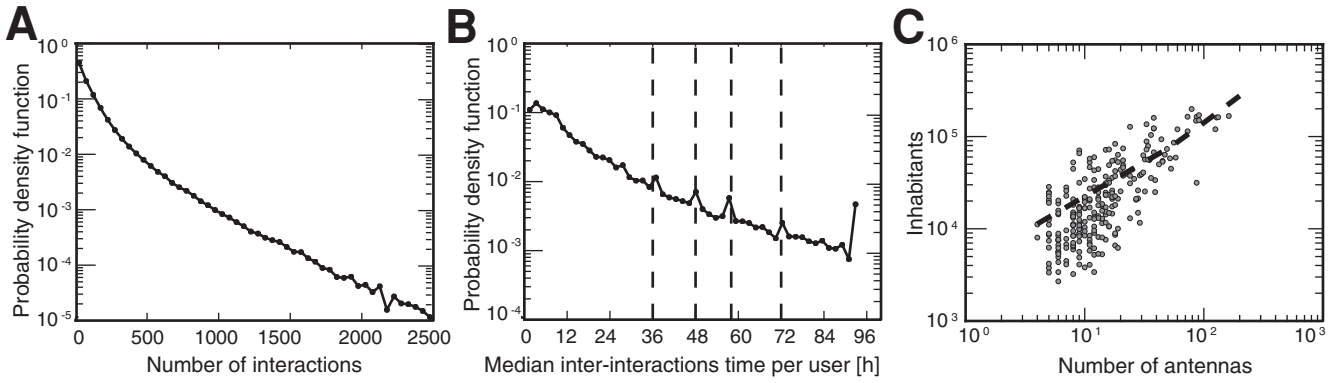


Figure 3 | (A) Probability density function of the amount of recorded spatio-temporal points per user during a month. (B) Probability density function of the median inter-interaction time with the service. (C) The number of antennas per region is correlated with its population ($R^2 = .6426$). These plots strongly emphasize the discrete character of our dataset and its similarities with datasets such as the one collected by smartphone apps.

www.nature.com/scientificreports

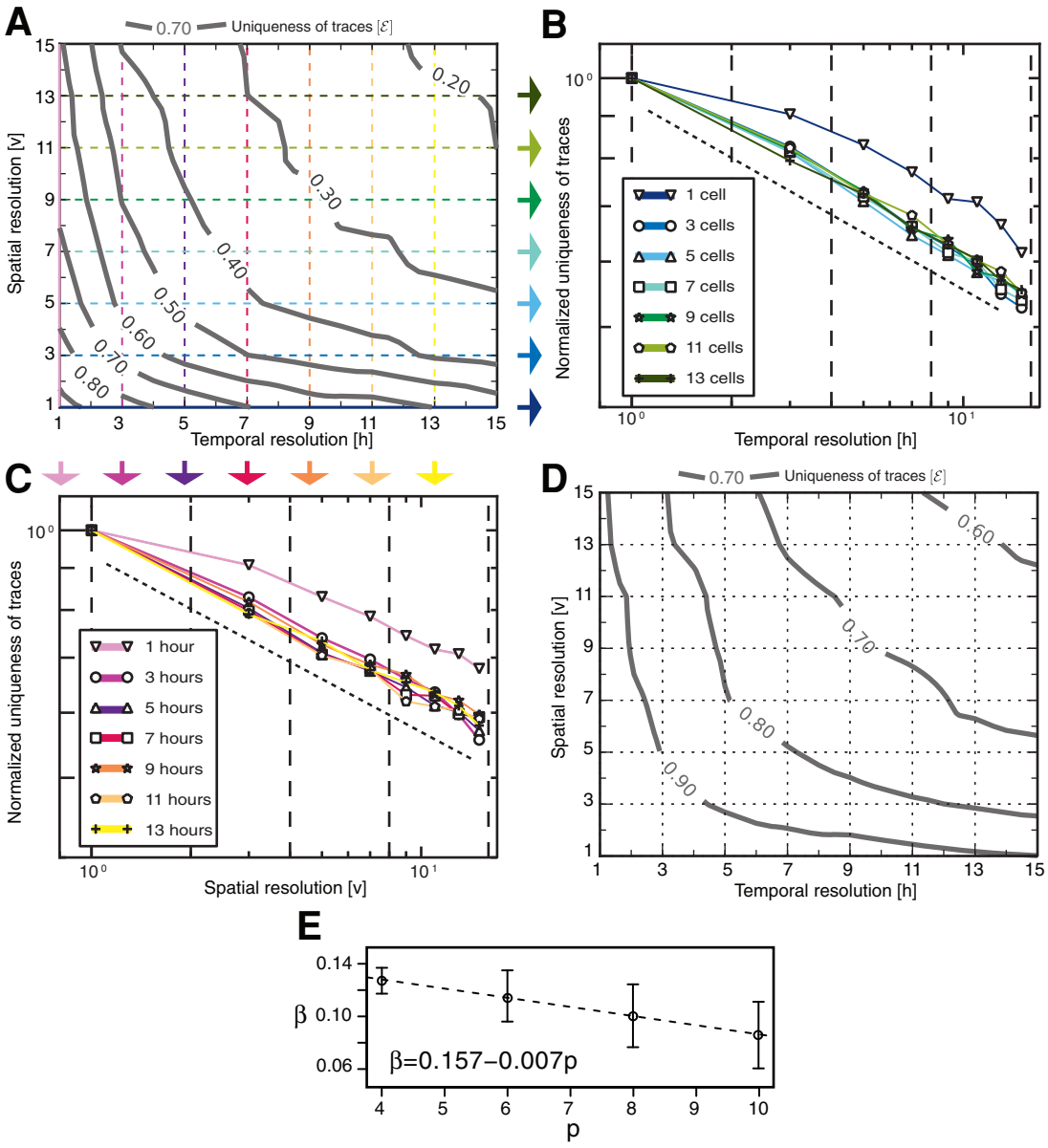


Figure 4 | Uniqueness of traces [ε] when we lower the resolution of the dataset with (A) $p = 4$ and (D) $p = 10$ points. It is easier to attack a dataset that is coarse on one dimension and fine along another than a medium-grained dataset along both dimensions. Given four spatio-temporal points, more than 60% of the traces are uniquely characterized in a dataset with an $h = 15$-hours temporal resolution while less than 40% of the traces are uniquely characterized in a dataset with a temporal resolution of $h = 7$ hours and with clusters of $v = 7$ antennas. The region covered by an antenna ranges from 0.15 km^2 in urban areas to 15 km^2 in rural areas. (B–C) When lowering the temporal or the spatial resolution of the dataset, the uniqueness of traces decrease as a power function $\varepsilon = \alpha - x^{\beta}$. (E) While ε decreases according to a power function, its exponent β decreases linearly with the number of points p. Accordingly, a few additional points might be all that is needed to identify an individual in a dataset with a lower resolution.

entropy is 1.74, less than two locations[18]. This makes our random choices of points likely to pick the user's top locations (typically "home" and "office"). Temporally, the distribution of calls during the week is far from uniform [Fig. S1] which makes our random choice more likely to pick a point at 4PM than at 3AM. However, even in this case, the traces we considered that are most difficult to identify can be uniquely identified knowing only 11 locations [Fig. 2C].

For the purpose of re-identification, more sophisticated approaches could collect points that are more likely to reduce the uncertainty, exploit irregularities in an individual's behaviour, or implicitly take into account information such as home and work-place or travels abroad[29,33]. Such approaches are likely to reduce the number of locations required to identify an individual, vis-à-vis the average uniqueness of traces.

We showed that the uniqueness of human mobility traces is high, thereby emphasizing the importance of the idiosyncrasy of human movements for individual privacy. Indeed, this uniqueness means that little outside information is needed to re-identify the trace of a targeted individual even in a sparse, large-scale, and coarse mobility dataset. Given the amount of information that can be inferred from mobility data, as well as the potentially large number of simply anonymized mobility datasets available, this is a growing concern. We further showed that while $\mathcal{E} \sim (vh)^{\beta}$, $\beta \sim -p/100$. Together, these determine the uniqueness of human mobility traces given the traces' resolution and the available outside information. These results should inform future thinking in the collection, use, and protection of mobility data. Going forward, the importance of location data will only increase[34] and knowing the bounds of individual's privacy will

J.A. 1478

be crucial in the design of both future policies and information technologies.

Methods

The dataset. This work was performed using an anonymized mobile phone dataset that contains call information for ~1.5 M users of a mobile phone operator. The data collection took place from April 2006 to June 2007 in a western country. Each time a user interacts with the mobile phone operator network by initiating or receiving a call or a text message, the location of the connecting antenna is recorded [Fig. 1A]. The dataset's intrinsic spatial resolution is thus the maximal half-distance between antennas. The dataset's intrinsic temporal resolution is one hour [Fig. 1B].

Unicity test and the likelihood of deductive disclosure. The considered dataset contains one trace T for each user. The traces spatio-temporal points contain the region in which the user was and the time of the interaction. We evaluate the uniqueness of a trace given a set I_p of p randomly chosen spatio-temporal points. A trace is said to be to be compatible with I_p if $I_p \subseteq T$ [Fig. 2A]. Note that this notion of compatibility can easily be extended to noisier or richer data. A brute force characterization is performed by extracting from the entire dataset of 1.5 M users $S(I_p)$, the set of users whose mobility traces T are compatible with I_p. All mobility traces in the dataset T are successively tested for compatibility with I_p. A trace is characterized "out of x", if the set of traces that are compatible with the points contains at most x users: $|S(I_p)| \leq x$. A trace is uniquely characterized if the set contains exactly one trace: $|S(I_p)| = 1$. The uniqueness of traces is estimated as the percentage of 2500 random traces that are unique given p spatio-temporal points. The p points composing I_p are taken at random among all the interactions the user had with the service. As discussed, we do not apply any constraints regarding the choice of I_p.

Minimum number of spatio-temporal location needed to uniquely characterize every trace. Fig. 2B shows that $.95 < \varepsilon < 1$ given $I_{p=4}$. Fig. 2C evaluates the minimum p needed to uniquely characterize every trace in a given set. This set contains a random sample of 1000 heavy-users, i.e. users that used their phone at least 75 times per month as their randomly chosen points might make their trace less unique.

Spatial aggregation. Spatial aggregation is achieved by increasing the size of the regions in which the user is known to be during his interactions with the service. In the case of discrete data, a bijective relation exists between antennas (known in this case as centroids) and the region defined by the Voronoi tessellation. The tessellation is defined so that every point in a region is closer to the region's antenna than to any other antenna. In order to increase the region's area, one should group antennas into clusters of a given size v. While the problem of optimally grouping places in a 2D space into groups of given sizes v is non trivial, it can be approximated through clustering methods. The canonical clustering methods focus on minimizing the within-cluster sum of squares rather than producing balanced clusters. This drawback can be controlled by the use of a Frequency Sensitive Competitive Learning scheme[35]. Fig. S2 shows the resulting group size histogram optimized for clusters of size 4. Once antennas are aggregated into groups, their associated regions are merged.

1. Clippinger, J. In *Rules for Growth: Promoting Innovation and Growth Through Legal Reform* (Kauffman Foundation, Kansas City, 2010).
2. Clanchy, M. T. *From Memory to Written Records England 1066–1307* (Harvard University Press, Cambridge, 1979).
3. Warren, S. & Brandeis, L. The right to privacy. *Harvard Law Review* **193**, 193–220 (1890).
4. Hey, T., Tansley, S. & Tolle, K. (eds) *The Fourth Paradigm: Data-Intensive Scientific Discovery* (Microsoft Research, Redmond, 2009).
5. Barabasi, A.-L. The origin of bursts and heavy tails in human dynamics. *Nature* **435**, 207–211 (2005).
6. Clauset, A. & Eagle, N. Persistence and periodicity in a dynamic proximity network. *Proc. DIMACS* (2007).
7. Eagle, N., Macy, M. & Claxton, R. Network diversity and economic development. *Science* **328**, 1029–1031 (2010).
8. Eagle, N., Pentland, A. & Lazer, D. Inferring social network structure using mobile phone data. *Proc. Natl. Acad. Sci. U.S.A.* **106**, 15274–15278 (2009).
9. Eagle, N., de Montjoye, Y.-A. & Bettencourt, L. Community computing: Comparisons between rural and urban societies using mobile phone data. *Computational Science and Engineering* **4**, 144–150 (2009).
10. Reader, T. *et al.* Predictors of short-term decay of cell phone contacts in a large scale communication network. *Social Networks* **33**, 245–257 (2011).
11. Hidalgo, C. & Rodriguez, C. The dynamics of a mobile phone network. *Physica A* **387**, 3017–3024 (2008).
12. Newman, M. E. J. *Networks: An Introduction* (Oxford University Press, New York, 2010).
13. Onnela, J.-P. *et al.* Structure and tie strengths in mobile communication networks. *Proc. Natl. Acad. Sci. U.S.A.* **104**, 7332–7336 (2007).
14. Szell, M., Lambiotte, R. & Thurner, S. Multirelational organization of large-scale social networks in an online world. *Proc. Natl. Acad. Sci. U.S.A.* **107**, 13636–13641 (2010).
15. Meloni, S. *et al.* Modeling human mobility responses to the large-scale spreading of infectious diseases. *Sci. Rep.* **1**, 62 (2011).
16. Balcan, D. *et al.* Multiscale mobility networks and the spatial spreading of infectious diseases. *Proc. Natl. Acad. Sci. U.S.A.* **106**, 21484–21489 (2009).
17. Gonzalez, M., Hidalgo, C. & Barabasi, A. Understanding individual human mobility patterns. *Nature* **453**, 779–782 (2008).
18. Song, C., Qu, Z., Blumm, N. & Barabasi, A. Limits of predictability in human mobility. *Science* **327**, 1018–1021 (2010).
19. Finding places on the go has never been easier. http://blog.foursquare.com/2012/02/08/finding-places-on-the-go-has-never-been-easier-%E2%80%93-check-out-the-new-explore-for-your-phone/, Accessed 2012 Jul. 1.
20. Blumberg, A. & Eckersley, P. On locational privacy and how to avoid losing it forever. *E.F.F.* (2009).
21. Apple privacy policy, http://www.apple.com/legal/privacy/, Accessed 2011 Jul. 25.
22. Federal reserve financial services federal reserve study shows more than three-quarters of non-cash payments are now electronic. *Federal Reserve* (2010).
23. Skyhook wireless spotRank overview, Available: http://www.skyhookwireless.com/location-intelligence/, Accessed 2012 Jul. 17.
24. Apples app store downloads top 25 billion, http://www.apple.com/pr/library/2012/03/05Apples-App-Store-Downloads-Top-25-Billion.html, Accessed 2012 Mar. 28.
25. The app genome project. http://blog.myLookout.com/, Accessed 2011 Jul. 27.
26. Mobile geo-location advertising will be a big number in 2015. http://adfonic.com/wp-content/uploads/2012/03/geo-location-white-paper.pdf, Accessed 2012 Jul. 17.
27. Sweeney, L. k-anonymity: a model for protecting privacy. *Int. J. Uncertainty Fuzziness and Knowledge-Based Systems* **10**, 557–570 (2002).
28. Zang, H. & Bolot, J. Anonymization of location data does not work: A large-scale measurement study. *Proc. Int. Conf. on Mobile computing and networking* **17**, 145–156 (2011).
29. Narayanan, A. & Shmatikov, V. Robust de-anonymization of large sparse datasets. *IEEE Trans. Secur. Priv.* **8**, 111–125 (2008).
30. Locard, E. Traité de criminalistique. (J. Desvigne et ses fils Lyon, 1931).
31. Boom! Foursquare crosses 2 million users. http://techcrunch.com/2010/07/10/foursquare-crosses-2-million-users/, Accessed 2010 Aug. 25.
32. Bates, D. & Watts, D. *Nonlinear Regression Analysis and Its Applications* (Wiley, Hoboken, 1988).
33. Golle, P. & Partridge, K. On the anonymity of home/work location pairs. *Pervasive Computing* 390–397 (2009).
34. Manyika, J. *et al.* Big data: The next frontier for innovation, competition and productivity. *McKinsey Global Institute* (2011).
35. Grossberg, S. Adaptive pattern classification and universal recoding: I. Parallel development and coding of neural feature detectors. *Biol. Cybern.* **23**, 121–134 (1976).

Acknowledgements

We thank Damien François, Janos Kertesz, Renaud Lambiotte, Vincent Traag and Paul Van Dooren for discussions and comments on the manuscript as well as Maxime Melchior for sharing computer code and Susie Fu for help with the figures. This work was supported by a grant 09/14-017 "Action de Recherche Concerté" of the "Communauté française de Belgique" on Information Retrieval in Time Evolving Networks.

Author contributions

Y.-A. de M. designed and performed experiments, analyzed data and wrote the paper; C.A.H. designed experiments, developed analytic tools and wrote the paper; M.V. and V.D.B. designed experiments and wrote the paper.

Additional information

Supplementary information accompanies this paper at http://www.nature.com/scientificreports

Competing financial interests: The authors declare no competing financial interests.

License: This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/3.0/

How to cite this article: de Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. & Blondel, V.D. Unique in the Crowd: The privacy bounds of human mobility. *Sci. Rep.* **3**, 1376; DOI:10.1038/srep01376 (2013).

Google, Android and Location Tracking

September 2018

Executive Summary

Google voraciously collects all manner of user data from its various products and services, including highly sensitive location data, and it takes extraordinary steps to both enable and preserve its ability to collect this information. On Android, turning off all services that track location is a complicated endeavor, and keeping them off is even harder. However, even if a user is able to navigate through the maze of options to successfully turn off the location services Google permits to be turned off, Google still collects location information. For example, Google openly admits to collecting the Internet Protocol (IP) address of devices – regardless whether location is on or off – and Google makes clear that a user's IP address reveals a user's location.

By spreading location related settings across multiple screens and services, Google makes it extremely difficult to turn all location related services off. When setting up a new Android device, users must navigate an opaque, intentionally difficult, and time-consuming process to determine the impact of each location service setting, all of which require users to "opt out" as opposed to "opt in." Further, any effort to maintain their "opt out" location services status is frustrated by a constant prompting to turn location services back on.

This paper reviews the location preferences that Google disperses across different settings and the impact of user choices at account and device levels. Second, we detail how these various location services are not opt-in: each is enabled by default and therefore provides the greatest benefit to Google instead of enabling user privacy. Third the paper reviews how, despite user choices that appear to limit location tracking, Google still collects information that is used to determine user location.

1) How Google Collects Location Data

Google's Android operating system nests location controls under multiple different settings (Figure 1). In order to make informed decisions regarding which location services to enable, users must first understand the differences between these settings. Furthermore a user must understand which of these settings have account-level or device-level effect.

Account-level settings operate independently of device-level settings. When a consumer adjusts an account-level setting, the new setting applies to all devices where the user is logged into her Google account (including Gmail, Google Chrome, Google Maps, YouTube, etc.). Any device level setting change is limited to the specific item of hardware where the consumer made the adjustment.

	DESCRIPTION	OPT-IN / OPT-OUT	USER CHOICES
LOCATION SERVICES	"**Use Google's location service to help apps** determine your location. Anonymous location data will be sent to Google when your device is on."	Opt-Out	"YES, I'M IN" or "SKIP"
LOCATION ACCURACY	**Three Modes** - "High accuracy", "Battery saving", and "Device only." **Default setting:** "High accuracy use[s] GPS, Wi-Fi, Bluetooth, or cellular networks to determine location"	Opt-Out	Toggle icon (right and colored for on, left and gray for off). This setting not shown during Android set-up.
LOCATION SCANNING	"**Improve location accuracy** by allowing apps and services to scan for Wi-Fi and Bluetooth, even when those settings are off."	Opt-Out	Toggle icon (right and colored for on, left and gray for off).
LOCATION HISTORY	"[A]llows Google to store a history of your location data from all devices where you are logged into your Google Account and have enabled Location Reporting. Location History and Location Reporting data may be used by any Google app or service."	Opt-Out	"YES, I'M IN" or "NO THANKS" In the context of "Give your new Assistant permission to help you"

Figure 1: Four Android settings and services that relate to location information collection. [1]

Google Location Services

Google Location Services (GLS) operate at a device level and rely on sensors such as GPS, Wi-Fi, the cellular radio, and other technologies included in mobile devices to position a user in the world. If a user keeps the default settings prompted by Google, Location Services is enabled, Location Accuracy will be set to "High Accuracy" [2]and Location Scanning will be enabled for both Wi-Fi base stations and Bluetooth Beacons, regardless of a user's choice to turn Wi-Fi or Bluetooth on. The implications of user choices among the various Location Services settings are significant, but not intuitive, including:

- With Location Services turned on, Location Accuracy set to "Device only" and Location Scanning turned off, an Android device will only use GPS to provide the location of an Android device.
- When Location Accuracy is set to "High accuracy" and Location Scanning is enabled (the default setting for new device setup), an Android device will use sources including Wi-Fi, Bluetooth, and cellular radio to improve the accuracy of the device's position.

[1] Location Accuracy and Location Scanning are additional sub-settings that rely on Location Services. If Location Services is turned off, users are unable to access Location Accuracy and Location Scanning settings. "Descriptions" explained here are taken from Google's own descriptions and prompts.

[2] Phone will use GPS, Wi-Fi, Bluetooth, or mobile networks to determine location.

- If Location Accuracy is set for "High accuracy" and Location Scanning is enabled, the Android device will also scan for Wi-Fi and Bluetooth signals even if a user toggles Wi-Fi and Bluetooth off on the Android device.[3] Collected Wi-Fi base station and Bluetooth beacon data is transmitted to Google to provide updated data for GLS.

Google Location History
Location History tracks a consumer across all of the devices they may use (a smartphone, PC, laptop, tablet, smart television, etc.) when logged into their Google account, such as when using a Google web service like Gmail. When enabled, a user's location and various characteristics about a user's movements over time are recorded and transmitted to Google.

Google "Web & App Activity" Settings
In addition to specific location-labeled settings, Google also operates a service that collects user data via its "Web and App Activity" setting. During an Android device setup process, Google enables this account-level setting by default. With Web and App Activity tracking, Google combines user behavior on the web, such as searches, across multiple devices, so long as those devices are signed in using the same account. While not disclosed during initial Android device setup, Web and App Activity settings also track user location via IP address, and via activities such as searching for a location on Google Maps.

2) Google Location Services are Not "Opt-In"

GLS, as presented to a user on an Android device, is not "opt-in" but is instead "opt-out", and is both difficult to disable and to keep disabled. Google claims that "users have the ability to opt into GLS when setting up their device or when using an application that uses GLS."[4] In fact, users are required to "opt-out" during the setup of an Android phone - Figure 2 displays screenshots taken during the initial setup process of an Android device by a new user.

Critically, and in direct contradiction to Google claims that users "opt-in" to GLS, Figure 2 clearly shows all setup choices to share location information with Google are pre-configured to the "on" setting – the canonical definition of user "opt-out." Rather than being asked to accept these preselected options, users are prompted to click "next." By clicking through this series of screens a user has, by default, set up their Android device to enable the constant monitoring of their location using GPS, sensor data, and information about things near the device, such as Wi-Fi MAC address and Bluetooth beacons.[5]

[3] https://qz.com/1169760/phone-data/
[4] Google's response to Senators Blumenthal and Markey, page 2, paragraph 5
[5] https://policies.google.com/privacy#infocollect

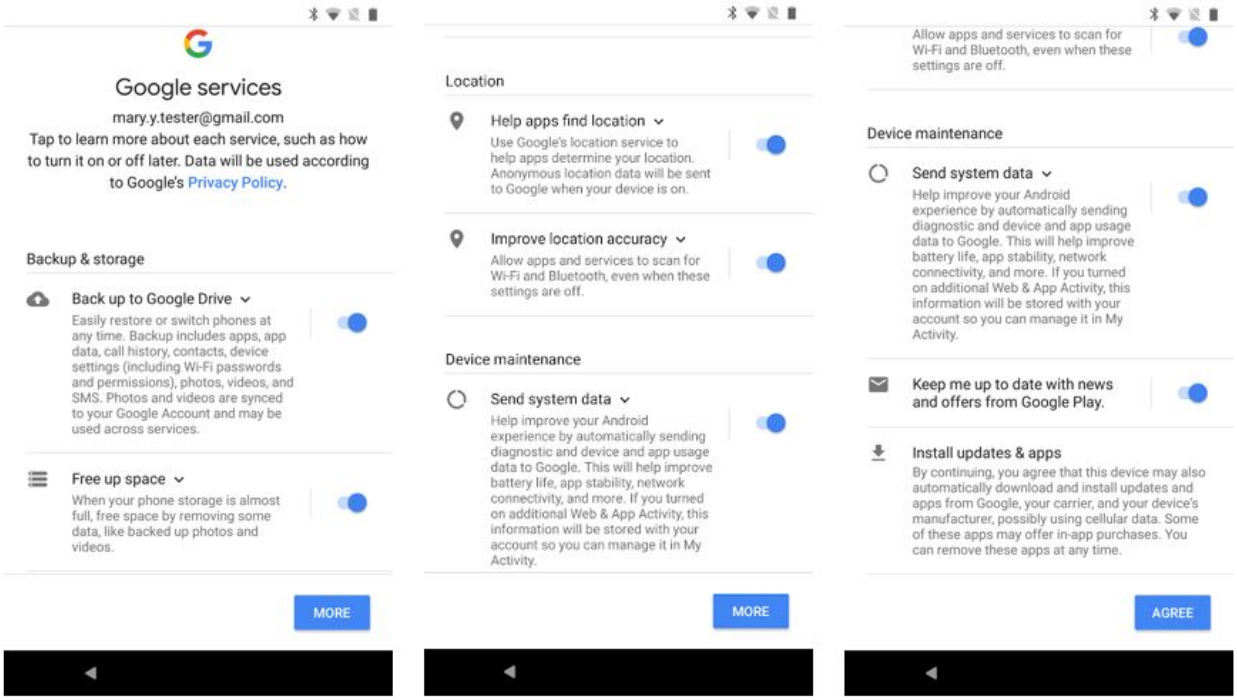


Figure 2: Google Services Defaults During Android Device Setup

Continuing through the Android smartphone setup process, users are prompted to enable **Google Assistant**[6] – a step that enables Location History, collection of device information, and recording of voice and audio activity of the user. Figure 3 displays the screenshots for setup of the Google Assistant service, bundling multiple settings with one "Yes I'm In". These default settings for Google Assistant also meet the criteria for an "opt-out" process, in direct conflict with Google's statement that "users must opt-in to this service."[7]

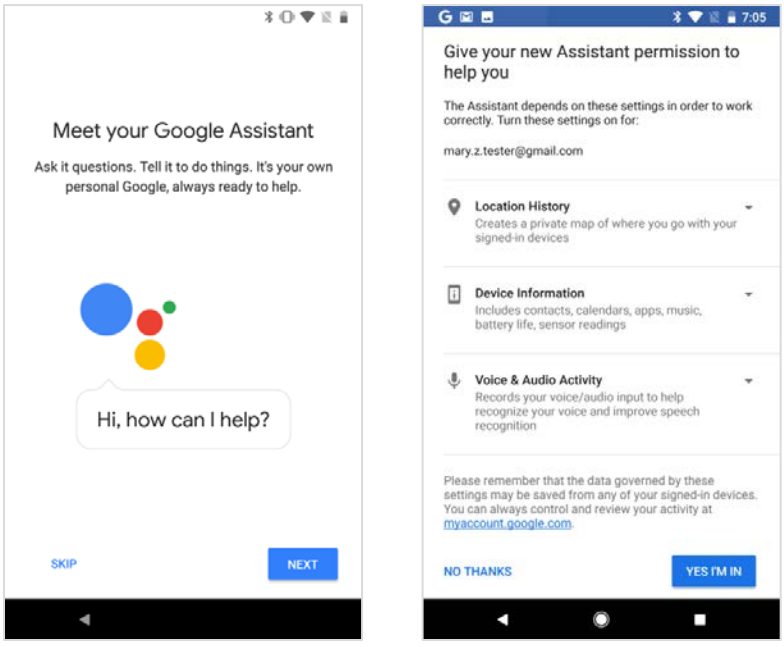


Figure 3: Google Assistant Setup Screens

[6] https://assistant.google.com
[7] Google's response to Senators Blumenthal and Markey, page 8, paragraph 5

After completing the setup process users can validate and control settings for device location via the Settings app and navigating to Google settings, then Location (Figure 4).

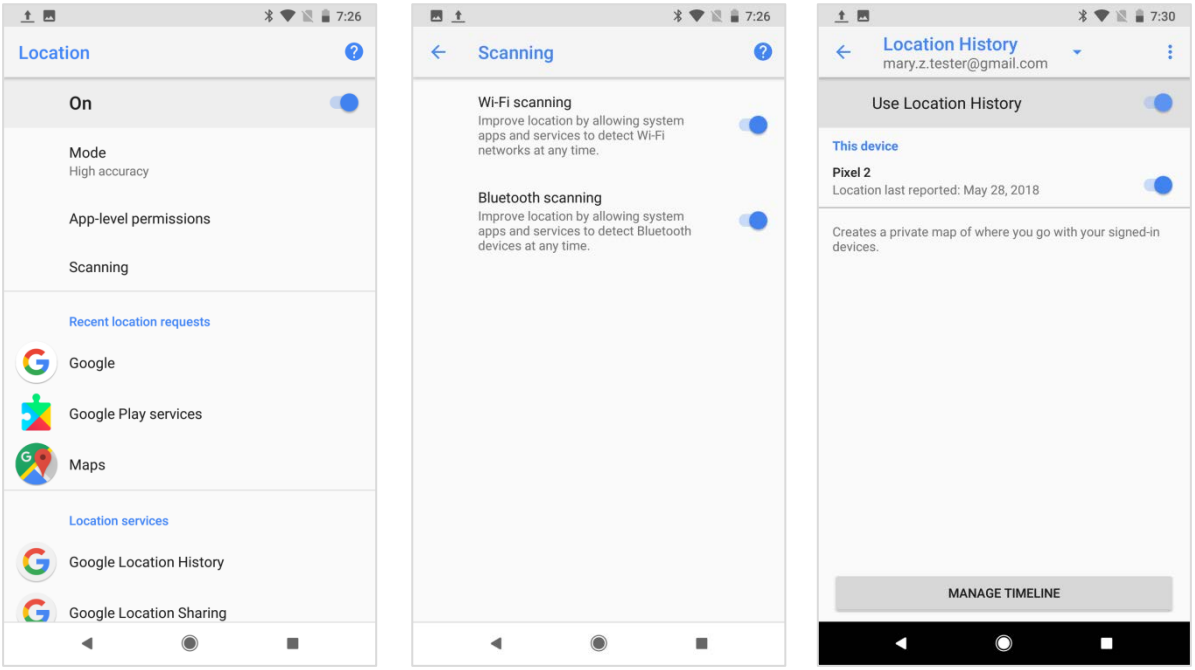


Figure 4: Location settings after Android device setup process

As demonstrated in Figure 4, if users accept Google's defaults during the setup process, the Android device is configured with Location Services enabled, Wi-Fi and Bluetooth scanning engaged, and Location History active.

Users can choose to disable GLS during the set-up process. However, if a user attempts to disable GLS, a warning dialogue box prompts an extreme scenario: "device location for all apps is turned off and you may not be able to locate your device if it is lost." (Figure 5) Note as well, the action prompt is to "Turn on Location" – reversing the user choice triggering the warning. Further, as described immediately below, many Google and third party apps will not function unless GLS is turned on. Therefore, Google forces user into an impossible ultimatum, have their every move constantly monitored, tracked, and stored or lose the functionality of their expensive smartphone.

If a user disables Location Services but then attempts to use a location aware app or service on their device, she will see the dialogue box shown in Figure 6. If the user clicks "OK" the service is enabled for the entire device and permanently, rather than enabling Location Services only for that particular app or service requesting the functionality.

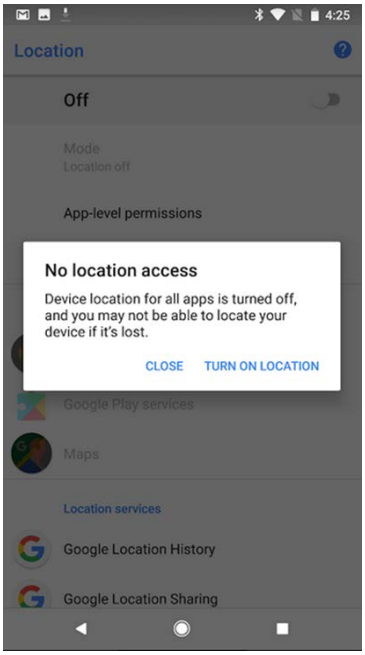


Figure 5: Location Services Warning

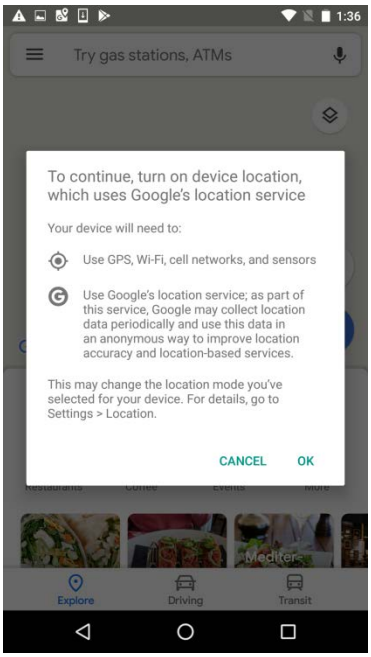


Figure 6: Re-Enable Location Services

Location History is treated in a similar manner by Google. Figure 7 highlights how the first time the Google Map app is launched, Google prompts the user to enable Location History if it is disabled. The user has two options, "Yes, I'm in" or "Skip," and they are informed that "Google needs to periodically store your location." It is worth noting that "Yes, I'm in" is highlighted by default and the "Skip" button blends in to the background of this screen. If the user selects the highlighted option, they have just turned on Location History universally across all devices associated with their Google account.

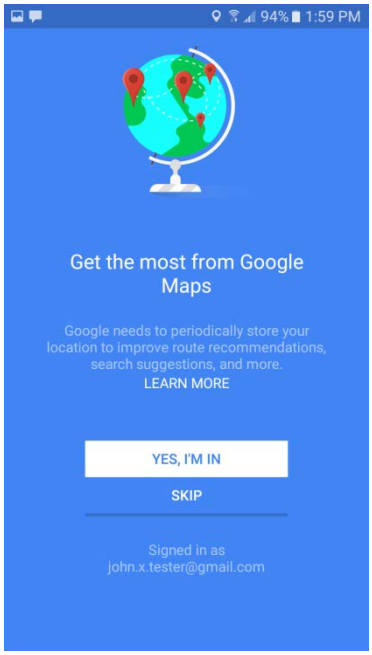


Figure 7: Location History Prompt

When adjusting the Location History setting, is it reasonable to expect that when Location History is disabled on one device, Google will not collect and store historical location on a user from that device. In practice, however, this is not the case. The Associated Press recently reported that Google in fact tracks historical locations of users who have Location History disabled on their smartphones. [8] This location tracking is a result of Google *also* tracking and storing user location across devices through its "Web and App Activity" settings. This setting is enabled by default to collect information across devices on an account (Figure 8).

[8] https://apnews.com/828aefab64d4411bac257a07c1af0ecb

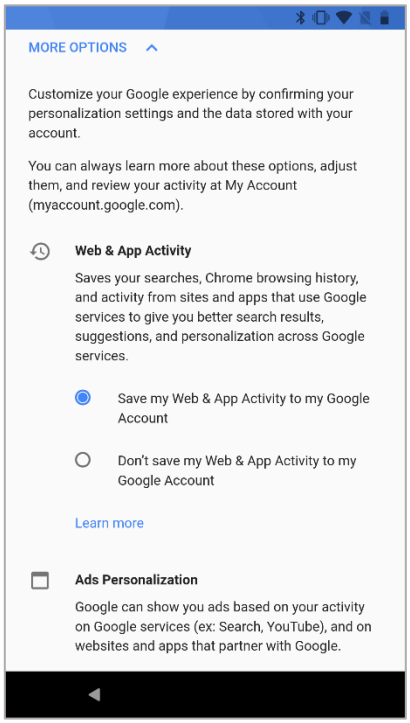


Figure 8: Web & Activity Setup Defaults

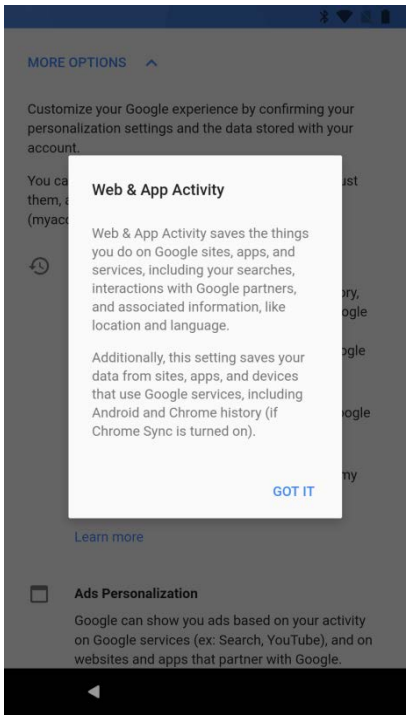


Figure 9: User Location Tracking Not Disclosed to User

Critically, the "Web & App Activity" setting does not disclose location tracking during the setup process, even if a user selects the "learn more" link (Figure 9). If the user has separate access to the internet and wishes to learn more than two sentences presented during setup about "Web & App Activity," they can review their Google Account Activity Controls and after digging through the site making three more navigation choices, they will learn what is saved as a result of enabling the setting (Figure 10). [9]

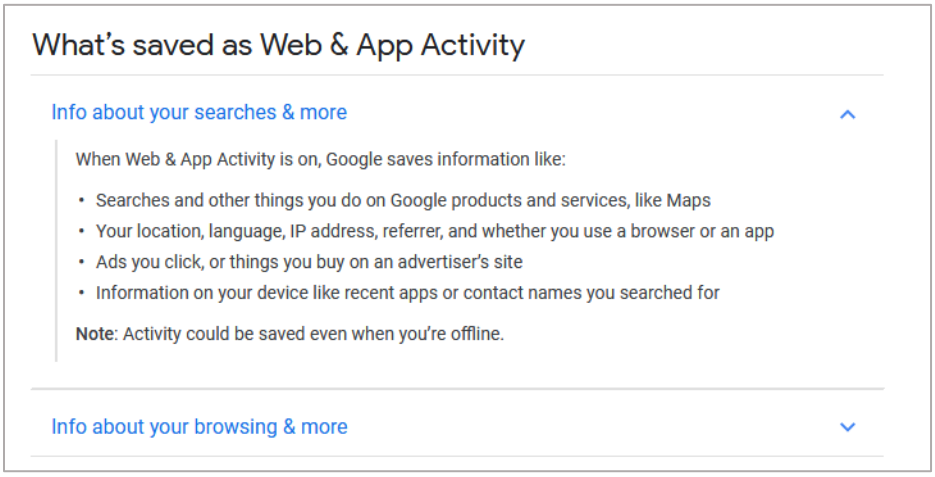


Figure 10: It takes multiple clicks to learn Google tracks your location with this setting.

[9] https://support.google.com/websearch/answer/54068?p=web_app_activity&co=GENIE.Platform%3DAndroid&oco=1

In response to an Associated Press report Google modified language detailing what happens when a consumer changes their Location History setting (Figure 11). Despite the first sentence claiming "You can turn off Location History at the account level at any time," Google goes on to disclose location data will continue to be collected and saved by Google. These statements are at best confusing, providing consumers with the illusion of control, while redefining the term "off" to mean "on."

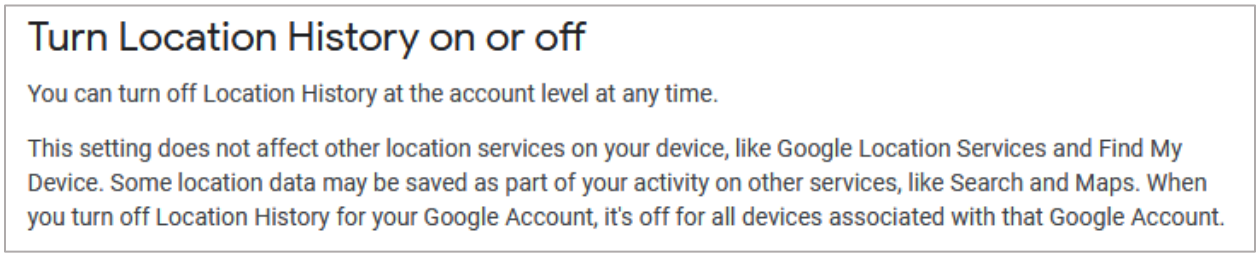


Figure 11: Google's Updated Disclosure (after Associated Press report) [10]

According to Google, a user can turn "Web and App Activity" on or off by taking the following steps (Figure 12):

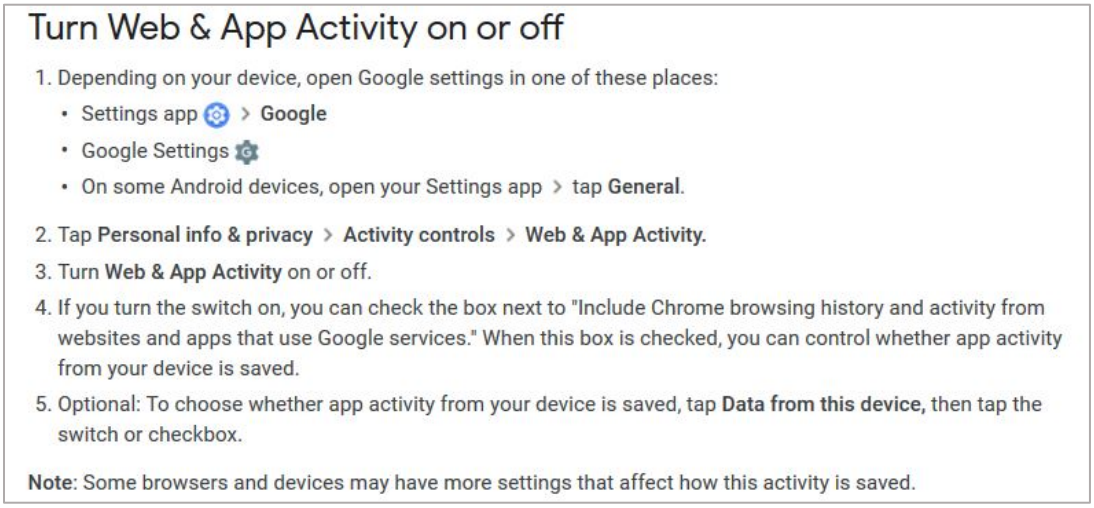


Figure 12: Google's Instructions for Web & App Activity Control [11]

In contrast, the six screenshots of Figure 13 reflect the *actual* steps an Android user must take in order to change their "Web and App Activity" settings, which when enabled also track, store and send a user's location to Google. [12]

[10] https://support.google.com/accounts/answer/3118687?p=privpol_lochistory&visit_id=636703138939910406-3172221135&rd=1

[11] https://support.google.com/websearch/answer/54068?p=web_app_activity&hl=en&authuser=0&visit_id=636699552478272972-2174117461&rd=1&co=GENIE.Platform%3DAndroid&oco=1

[12] Screenshots taken on 16 August 2018 on an Google Pixel 2 running Android 8.1.0

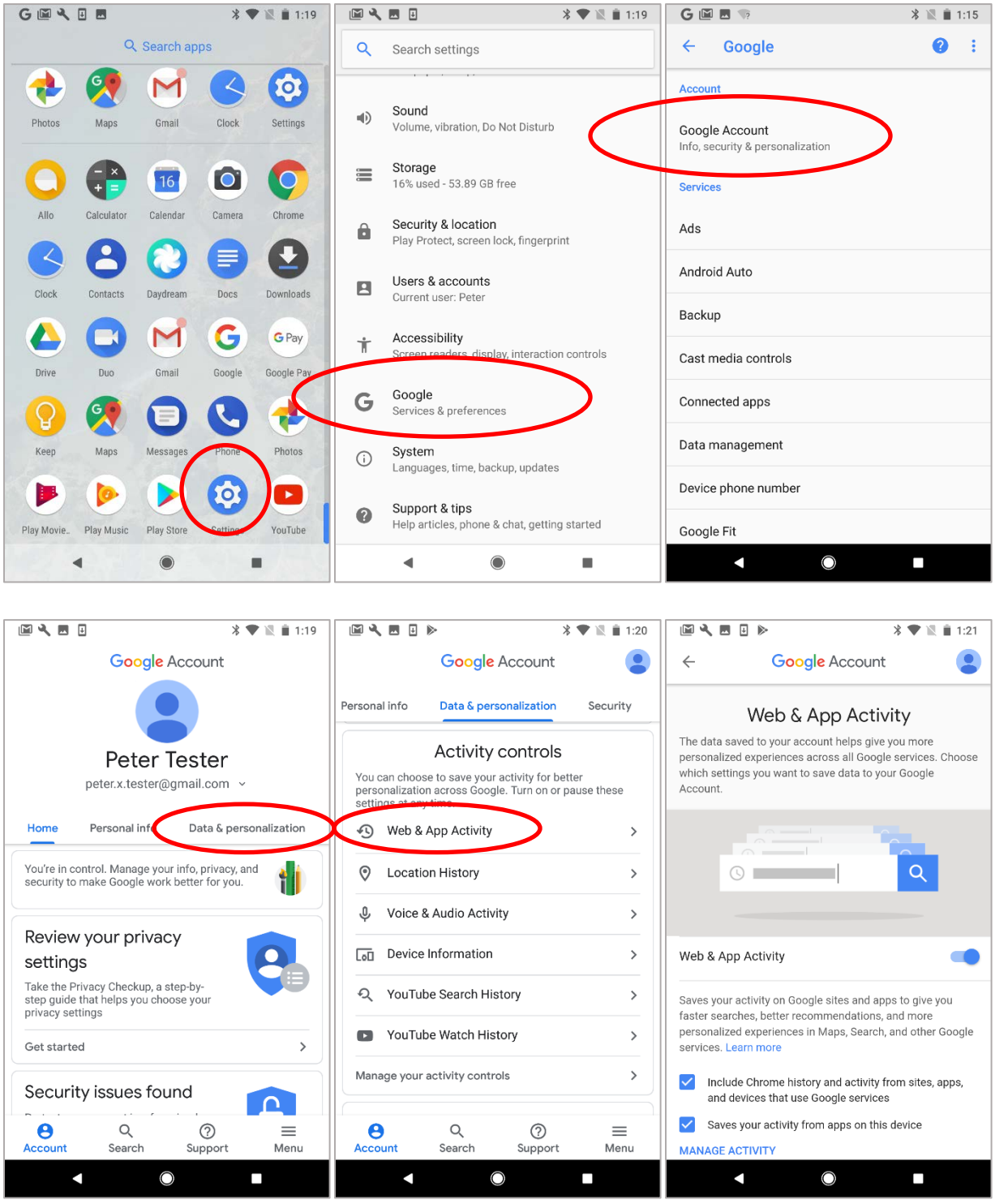


Figure 13: User steps to change Web and App Activity setting

3) Users are unable to turn off all location tracking on an Android device.

Google incorrectly claims that a user can turn off location tracking on an Android device. Even if a user is able to navigate through various opaque and intentionally difficult opt-out processes, they will be unable to prevent location tracking of their Android device. Irrespective of whether a user may toggle Google's Location Services on or off in the Settings app (Figure 4), Google continues to collect Internet Protocol (IP) addresses, which, according to Google's privacy policy[13], it uses to determine "the location from which a device is connecting to the internet." (Figure 14)

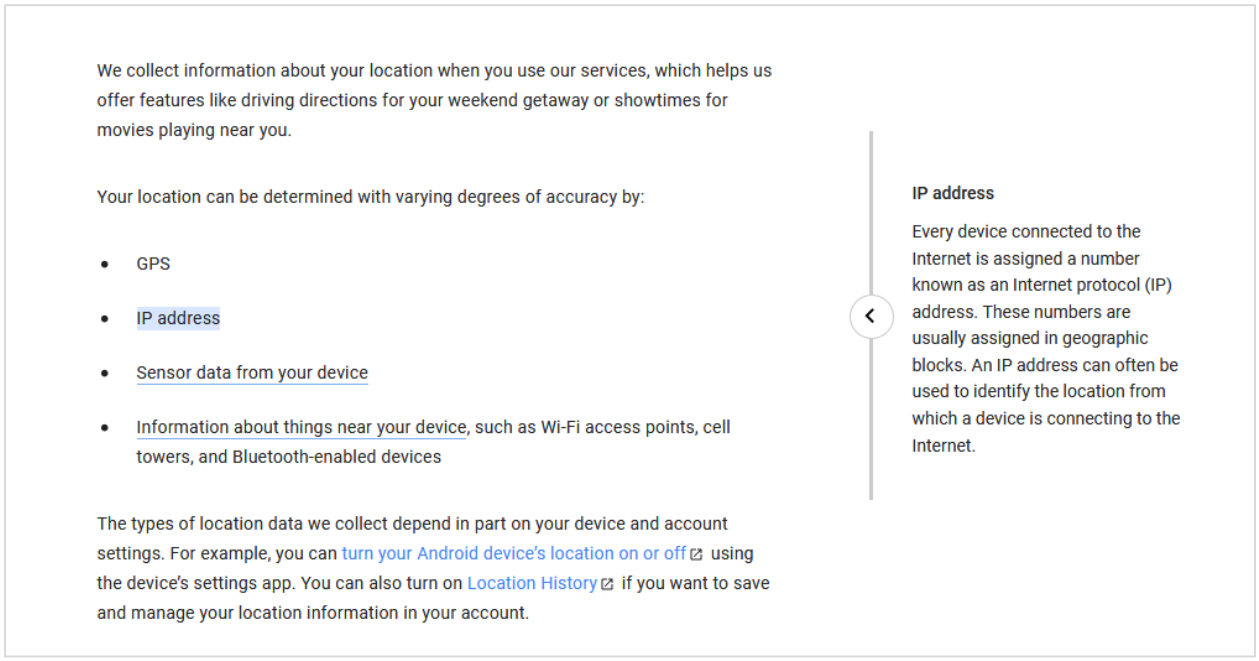


Figure 14: Portion of Google Privacy Policy Detailing IP Address Based Location Determination [14]

Google further confirms that it uses IP addresses to track a user's location through a disclosure made by Google's Vice President of Public Policy and Government Relations for the Americas, Susan Molinari in her letter to Senators Blumenthal and Markey (Appendix A). In that response, she states that Google continues to track consumer location for advertising through geolocation of IP addresses. She explicitly states, "We collect and use various types of location information in our products" [15] and then specifies that Google will "use a user's IP address to identify their general location." [16] This location data is then used by Google to target ads, as detailed in their own words: "Google uses location information in our ads products to infer demographic information, to improve the relevance of the ads users see, to measure ad

[13] https://policies.google.com/privacy/update
[14] https://policies.google.com/privacy#footnote-ip
[15] Google's response to Senators Blumenthal and Markey, page 2, paragraph 3
[16] Google's response to Senators Blumenthal and Markey, page 5, paragraph 3

performance, and to report aggregate statistics to advertisers. While our systems may use this information to show relevant ads, user location data is not shared with advertisers." [17]

Consumers are unable to control this behavior.

Android users are therefore unable to prevent the disclosure of their location to Google. Even if Google Location Services and Location History are disabled and they know enough to disable Web & App Activity settings, the IP address of Android devices will ***still*** be transmitted to Google. Again, Google notes that part of the operation of messaging and notification systems on Android, "it is important for a device to keep its connection alive for as long as possible", and as a result, "Android devices and servers send pings to each other (referred to as "heartbeats")." [18] These device "heartbeats" disclose the user's Android device IP address to Google independently of any location related user device settings. As such, Google can – and does - determine a user's location with Location Services disabled in order to target and sell ads.

Additional Consumer Activity Data Collected by Google

Google monetizes user data it collects for advertising purposes, [19] however, not all of the data sources Google collects are of equal value or sensitivity. Streams of user location and activity data from Android smartphones are uniquely valuable to Google, as they create detailed profiles of real-world behavior of individuals and their patterns of life. A second-by-second record of individuals every movement is highly sensitive, if not intimate, and permits Google to "close the loop," [20] tracking and targeting users with ads from the moment they wake and while they go about their daily routine.

Individuals are not likely to turn off location services Google pre-selects, as evidenced by the fact that nine in ten US smartphone owners use location-based services on their phone. [21] If an Android user does manage to opt-out (and continue to remain so), Google continues to collect a vast array of information about an individual's online activity [22] including:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services

[17] Google's response to Senators Blumenthal and Markey, page 5, paragraph 3
[18] Google's response to Senators Blumenthal and Markey, page 7, paragraph 5 and 6
[19] https://www.sec.gov/Archives/edgar/data/1652044/000165204418000027/goog10-qq22018.htm
[20] https://adwords.googleblog.com/2016/09/New-Digital-Innovations-to-Close-the-Loop-for-Advertisers.html
[21] http://totalaccess.emarketer.com/Reports/Viewer.aspx?R=2001793&ecid=MX1086
[22] https://policies.google.com/privacy#infocollect

- Chrome browsing history you've synced with your Google Account
- Telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls

This information is collected independently of location information.



January 12, 2018

The Honorable Richard Blumenthal
United States Senate
706 Hart Senate Office Building
Washington, D.C., 20510

The Honorable Edward J. Markey
United States Senate
255 Dirksen Senate Office Building
Washington, D.C., 20510

Dear Senator Blumenthal and Senator Markey,

Thank you for your letter of December 1, 2017. We appreciate the opportunity to explain our products and practices and to provide more information about the press report you note.

Privacy and security are critical issues for Google and we are deeply committed to keeping user data private and secure.

We want to be clear, the Quartz story you reference mischaracterizes what happened and how our systems work. The system it described did not use cell tower identifiers (”Cell ID”) and never tracked user location. The Quartz article discussed device-side code that is part of a system Google uses to maintain a persistent connection between devices and servers so that the devices can receive notifications and messages in real-time. The system determines the optimal interval at which devices should “ping” servers so that this persistent connection stays open. If the connection closes, messages and notifications may be delayed and users would have to refresh their apps manually to get new messages. This system is designed to help users by determining the optimal ping interval, which helps preserve users’ device batteries and makes real-time messaging available.

The claims that Google was using Cell ID from these transmissions to track user location are unfounded and untrue. While the device-side code transmitted data including Mobile Country Code or “MCC”, Mobile Network Code or “MNC” and Cell ID, the server-side code (which would not have been accessible to the Quartz reporter) only logged MCC and MNC.

Although the Quartz article incorrectly stated that we were using Cell ID to track users’ locations, we do use location data that we collect in other contexts to provide useful products and features to our users such as Google Maps. We welcome the opportunity to answer your additional

questions about how Google and Android work, and have included responses to these questions below.

1. **Google's privacy policy asserts, "When you use Google services, we *may* [emphasis added] collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that *may* [emphasis added], for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers." Under what circumstances "may" Google collect this data? Under what circumstances does Google *always* collect this data? Under what circumstances does Google *never* collect this data?**

We collect and use various types of location information in our products. The types of information we collect depend on a number of factors, including the service we are providing and the user's settings.

For example, standard Internet traffic information, such as IP address, can be used to provide the user with the correct language and locale for search queries. Some products, such as turn-by-turn navigation in Google Maps for mobile, use more precise location information such as GPS signals, device sensors, and Wi-Fi access points when the user has enabled device-based location services.

The Google Location Service (GLS) is the platform network location provider for most Android devices. GLS collects certain kinds of location information (such as Wi-Fi and GPS) from users who have opted into this service on their device and uses that information in an anonymized manner to help improve location accuracy and location-based services. This information also helps determine a device's location, which can be provided to applications that have the necessary location permissions. Users have the ability to opt into GLS when setting up their device or when using an application that uses GLS, and may subsequently disable this collection in their device's location settings at any time.

Location History is a different, Google account-level setting that allows users to store their location information with their Google account in order to get better results and recommendations across Google products. For example, users can see recommendations based on places they have visited with signed-in devices, or traffic predictions for their daily commute. Location History is off by default, and users must opt-in to turn on Location History for their Google account. Users have the ability to control their historical locations saved in their Location History, and can delete all or part of that history at any time.

   a. **What do you mean by "when you use Google services?" Is *all* of Android's operating system a Google service?**

Google plays two roles with respect to data collected on Android. First, Google develops and releases the Android operating system under an open source license, enabling anyone to

access the Android source code and create modified versions of it. In addition, Google develops proprietary mobile applications and services such as Google Play, Search, and Maps (referred to as "Google Mobile Services," or “GMS”), and licenses them separately from Android, meaning that device manufacturers can choose whether and on which devices to install GMS (or can use another mobile OS or suite of comparable apps). These apps, like those created by other developers, run on Android and make use of the platform and other device information to provide services directly to users. The Android operating system on devices with Google apps is a Google service covered by Google’s Privacy Policy.

With respect to Android users, therefore, Google may receive information both from their use of Google apps, as well as Google applications installed on the device and services built into Android to make the platform and device function properly (such as the network sync system described below in question 8). Any personal information a user provides to Google, whether through Android system services or Google apps on Android, or that is otherwise generated and stored in a user’s Google Account, is used and protected in accordance with the Google Privacy Policy.

This does not mean, however, that Google collects and uses all of the information on an Android device. For example, much of the information that a typical user generates while using Android is collected solely by third party apps running on the platform. As another example, Google enables device manufacturers to modify the open-source Android software such that Google does not receive any information from users of these devices. Information collected by other developers would be subject to their own privacy policies, rather than Google’s.

b. What do you specifically mean by “nearby devices?”

With respect to your question on “nearby devices,” many connected devices, such as Wi-Fi routers and Bluetooth-enabled devices, are able to detect and connect with each other. Application developers, including Google, may be able to infer a user’s location through these connections. For example, if a user has opted into GLS, Google may use publicly broadcast Wi-Fi data from wireless access points in range of the device to help determine its location. As described in more detail below in response to question 5, only publicly broadcast Wi-Fi information is used to estimate the location of a device in this manner.

2. If a user goes "offline” and disconnects their mobile phone from the Internet for a period of time, or even places the device in so-called "airplane mode,” does Google receive location data, Wi-Fi data, cell tower data, during this "offline" time period, even if location services is still on?

“Airplane” or “offline” mode is a common setting for mobile devices that disables the device’s cellular antenna. When a device is switched into airplane mode, no cellular data, including cell tower data, is sent or received -- however, the device may contain information about the last cellular tower to which it was connected before airplane mode was enabled. A device’s Wi-Fi

radio is typically controlled by a separate setting that can be enabled even when a device is in airplane or offline mode, for example to connect to an airplane's Wi-Fi network, or to use the device over a hotel's Wi-Fi network when a user is traveling somewhere without cellular service.

Accordingly, if a user enables airplane or offline mode but leaves on the Wi-Fi radio and connects to a Wi-Fi network, they will be able to continue to send and receive data on their device, including location data, over the Wi-Fi connection. This may include the types of location information described above, depending on the user's settings and the products or services they are using.

3. **What location data does Google specifically collect from Android users and under what circumstances? Is the location data associated with a specific device ID? Is it associated with a specific user ID? Are there any other specific user or device identifiers involved?**

As described above in our response to question 1, the types of location information that Google collects depends on a number of factors, including the service being used and a user's settings. With respect to Android specifically, location information can be used to provide a range of functionality, such as automatic traffic predictions or better search results. Depending on whether and how they want to use these features, users have a number of options for how their location data is collected, including the ability to turn location mode on or off for the device, as well as changing the device's "location accuracy" setting, which controls the sources used to estimate the device's location.

The information Google collects from Android devices for use in GLS is linked to a temporary and rotating device identifier that is not used by or shared with other services. It is not connected with any identifier that would associate that data with a specific user. If a user has opted into Location History, as described above, this location data is stored with their account identifier. Users can control the specific location information saved in their Location History, and can delete their history at any time.

   a. **Can you please attach to your response examples of any relevant files or server logs transmitted by an Android device to Google so we can see for ourselves what location information is being compiled and transmitted?**

With respect to your request for examples of files or logs transmitted by an Android device, we are happy to organize a briefing to determine the specific information that might be most helpful to you.

4. **Is a user's specific location data combined with other information Google collects about users' Internet activities? Is it combined with search data? DoubleClick cookie data? YouTube data, etc.?**

We collect location information in many of our products, and use it along with other information to enhance and improve services for users, and do other things like detect fraud or improve security.

Google Search uses location data to make search results more relevant to the query and the user, and to select ads. For example, searches like “restaurants near me” depend on the device’s location to understand what nearby means at that moment. Similarly, a word like “football” usually means something different in the U.S. than it does in the U.K. Some features on the search results page link to licensed content, and for that we try to link the user only to content available in her country. Finally, we use location to serve more relevant ads to that user, similar to the uses for organic search results.

As we describe in our advertiser help center, Google’s ad products may receive or infer information about a user’s location from a variety of sources. For example, Google may use a user’s IP address to identify their general location; receive precise location from a mobile device; or infer a user’s location from search queries. In addition, websites or apps a user is using may send information about their location to us. Google uses location information in our ads products to infer demographic information, to improve the relevance of the ads users see, to measure ad performance, and to report aggregate statistics to advertisers. While our systems may use this information to show relevant ads, user location data is not shared with advertisers. For our ad services that operate on partner websites or apps, we may receive more precise location information in an ad request, but we use and store only the general area of the specified location.

YouTube uses a user’s location to both personalize the user’s watch and recommendations experience, to accurately serve the content licensed to YouTube by content providers, and to target ads. For instance, a user’s country will determine what videos they see on the “Trending” tab of YouTube. The “Trending” tab is a set of videos that are rising in popularity in that user’s country. For licensing restrictions, YouTube also allows many content owners to select which content is available in which countries. For example, when Disney changed the name of Zootopia to Zootropolis in the U.K., YouTube was able to serve the appropriate trailer to users in the U.K. Finally, as discussed above, YouTube uses a user’s location to serve more relevant ads to that user.

Google may also collect and use location information to help detect fraud or other suspicious activity on a user’s account. For example, users can review the dates and times on which their accounts have been accessed, as well as the IP address and general location from which these accesses occurred. This enables users to confirm their accounts have not been compromised when unusual activity -- such as an account access from a new country -- is detected.

5. **Regarding “Wi-Fi access points,” per your privacy policy, can you describe exactly what information is being collected and for what purpose? Are you collecting just known Wi-Fi access points a device has previously connected to or all Wi-Fi access**

points in range of the device? Are you collecting just network names or more information like a MAC ID, network address, signal strength or any other information? Are you collecting information about so-called "hot spots," other devices transmitting Wi-Fi signals? Are these Wi-Fi access points stored in a Google database and are they used for identifying a user's specific location?

Questions 5(a)-(c) are describing the GLS we provide as a network location provider on Android devices, which uses sources like Wi-Fi and mobile networks to give location information faster and more accurately. When setting up their device or using apps or services that can use location services, a user may enable GLS to take advantage of these features. GLS uses publicly broadcast Wi-Fi data from wireless access points in range of the device to help determine its location. This may include any Wi-Fi access points in range of the device, and not just networks to which the device has previously connected.

These access points are stored and used to build models that estimate where each access point is located. This data is de-identified and only associated with a temporary, rotating device identifier, and no payload data/data packets are collected. As noted above, only publicly broadcast Wi-Fi information is used to estimate the location of a device.

To provide this functionality, Google collects MAC addresses, signal strength information, and radio channel information from these access points. Google also collects the name (also referred to as a "service set identifier" or "SSID") associated with these networks, in order to identify and remove access points that network administrators have chosen to opt out of this collection through instructions provided by Google. SSIDs are discarded after being processed for this purpose.

6. **Are there other network signals you are collecting, such as Bluetooth beacons? Again, all Bluetooth signals or only known or paired Bluetooth beacons? Specific device identifiers? Signal strengths?**

The GLS described above does not use Bluetooth beacon information to determine location.

There are other Google products that may scan and collect certain information from Bluetooth beacons near the device. This includes information that any Bluetooth beacon may be publicly broadcasting for use, such as beacon type, beacon identifier, signal strength, and broadcast power. For example, if a user has turned on the opt-in Location History feature for their Google account, Google will use publicly available beacon information as one signal to help determine location. Other Google products, such as the Nearby service, use Bluetooth scanning to detect nearby Bluetooth beacons in order to show relevant notifications to users when they are near businesses, and other places that have installed Bluetooth beacons for this purpose.

7. **As you know, today's mobile devices contain a range of sensors and consumers may or may not be fully informed about the purpose of those sensors. For example,**

consumers believe accelerometers are primarily for tracking a users' "steps" within a health app. Do you collect accelerometer data to assist in location tracking? How often and under what circumstances? Consumers believe barometer information is primarily used for "weather" within a weather app. Do you collect barometer information to assist in location tracking? How often and under what circumstances?

Many Android devices have built-in sensors that measure motion, orientation, and various environmental conditions. The Android operating system supports a number of these different sensor types, which vary from device to device. These sensors are used to provide a variety of functionality to application developers, such as the ability to measure device movement or positioning to support motion-based games, or to report a compass bearing for a travel application.

Android application developers, including Google, can use the accelerometer and barometer sensors, along with the gyrometer and magnetometer sensors, to more precisely determine a device's location. Google uses the accelerometer readings to help determining the device's orientation and direction, the gyrometer helps determine if a user is turning, and the barometer can help determine the user's elevation.

8. **The Google spokesperson cited in the *Quartz* article stated that "we never incorporated Cell ID into our network sync system." Can you describe exactly what your network sync system is and what information is "incorporated" into it and for what purpose? Does the network sync system include other location-related information?**

The network sync system supports real-time messaging in Google and third party applications on Android mobile devices (*e.g.*, chat apps or notifications). Modern messaging and notification systems allow users to send and receive messages in real-time, so they do not have to "refresh" to see new messages. To do this, it is important for a device to keep its connection to servers alive for as long as possible. If the connection drops, messages will not arrive until the connection is re-established. And a device's battery power is drained when the device attempts to re-establish its connection to the server.

To keep this connection alive, Android devices and servers send pings to each other (referred to as "heartbeats"). If a device does not send a heartbeat ping after a certain period of time, the connection will terminate. For the benefit of users, Google seeks to determine the timing of these heartbeats that best balances the need to maintain a persistent connection between the device and the server with the preservation of device battery. If heartbeats are not frequent enough, connections are lost. If heartbeats are too frequent, battery power is depleted.

Mobile networks have different amounts of traffic and employ different technologies. These factors impact the optimal time interval to wait between each heartbeat. Thus, a device's mobile network provider will impact how frequently a device should send a heartbeat.

Knowing the network to which a device is connected helps Google determine how frequently a device should send a heartbeat ping. Google has access to mobile network information because the information that cell towers transmit to a device includes a MCC (indicating which country the tower is in), a MNC (indicating which cellular network operates the tower), as well as other information like a unique number assigned to each tower (Cell ID). In this instance, the device-side code on Android devices was designed to transmit information from the device that included all three of these data elements. The network sync system also relies on server-side code that determines what information Google actually logs on our servers in connection with the network sync system. This server-side code was written to only log MCC and MNC data for use in the network sync system. Once Google had the MCC and MNC from the device, we aggregated that information and used it to test different ping intervals per country and network in order to determine the optimal ping interval for each network and country.

This heartbeat "tuning" process was the sole reason Google collected the information transmitted by the device-side code at issue; this information was not used to determine user location. In fact, Google never used the Cell ID data from the transmissions to determine user location or, for that matter, ping intervals.

9. **As you know, Google provides metrics on "store visit conversions" -- meaning when a targeted ad translates into a retail store visit. These metrics are "calculated based on aggregated anonymized data from hundreds of millions of Google users who opt-in to share Location History, click on a search or display ad, then visit a business location." How is Google able to obtain this data if, as was claimed by a Google spokesperson, location data was never used or stored? Specifically, how does Google know when a user visits a business location with "99% accuracy"? Has this location data ever been used to determine if consumers visited a retailer or was influenced by an online/mobile advertisement? If not location, has any other data been used to determine consumer behavior? How exactly are consumers "opting in" to this kind of tracking and use of their data to inform Google store visits conversions?**

As explained, Cell ID information was never used to track user location. It is completely unrelated to our Store Visits measurement feature. The Store Visits feature allows retail advertisers to get anonymized and aggregated reports of visits to their retail locations by Google users who also clicked on an ad for the advertiser's products or services. Store visits are measured exclusively using data from Google users who have activated Location History, which provides a location timeline, stored against the user's Google Account. Google correlates the observed store visits from those users who have activated Location History with those users' ad clicks and then uses that data to estimate the aggregate number of store visits for all users who clicked on the advertiser's ads.

Location History is turned off by default, meaning that users must opt-in to this service. Timeline

gives users full control over the locations they choose to keep. Users can pause or delete location history at any time via Timeline.

We provide more information about Store Conversion services in our advertiser help center, which is available at: https://support.google.com/adwords/answer/6361305?hl=en.

10. **While you commit in the article to cease sending "cell-tower" location data to Google by the end of November, it is not clear if you are also committed to refraining from sending other forms of user location information -- whether determined by GPS, Wi-Fi access points, nearby devices, sensors, or any other kind of technology? Can you clarify?**

By the end of November 2017, Google deactivated the device-side code that transmitted the Cell ID to the network sync system, and that code was changed on each Android device the next time it checked in to receive updates.

As described in our previous answers, other forms of location data are collected and used by Google outside the network sync system, to provide a variety of product and service features.

11. **Does Google collect user data from Apple iOS devices through Google apps? If so, what data is collected from iOS devices? How is that data collected? Does Google recognize and respect all of the privacy choices made by iOS users? Is Google confident that it is not inadvertently collecting data from consumers who have affirmatively opted out of data collection or location sharing? For example, if a consumer is using Google maps on an Apple device, does Google receive and store that location information?**

Google provides a number of applications for iOS devices, which collect information consistent with Google's Privacy Policy, user controls, and iOS platform rules and settings, including those pertaining to location data.

12. **Does anyone pay for location-related data transmission when a consumer is not using a specific app or not using the Internet? If yes, please identify the parties. Is this location data transmitted over the cell network, where a consumer is paying for the data? Or just when a user is connected to Wi-Fi? How much information is being transmitted that is not related to a users' specific app or Internet usage and is not for the purposes of diagnostics?**

Data sent and received from Android devices may be transmitted over a Wi-Fi network or over the device's cellular connection. In the case of mobile devices, any charges for transmission of data over a cellular connection -- including any location-related data -- would be governed by a user's mobile carrier plan. The types and quantity of such data that a user's device transmits would depend on the products or services they use, and, in some cases, a user's settings.

Like all operating systems, Android collects diagnostic and other data from user devices to provide and improve system services and device functionality. As we describe above, one such function is the network sync system, which periodically exchanges pings between mobile devices and Google's servers. This helps to maintain a persistent connection so that the devices can send and receive notifications and messages in real-time without having to re-connect to Google's server and deplete battery power.

We appreciate the chance to clarify what happened and how our systems work, as well as explain Google's products and privacy practices. Protecting the privacy and security of our users is a top priority and we thank you for the opportunity to further underscore our commitments in these areas. Please let us know if we can address any other questions you might have or be a resource to you on our shared goals of improving users' mobile experiences and protecting users' privacy and security.

Sincerely,



Susan Molinari
Vice President, Public Policy and Government Relations, Americas
Google

AO 106 (Rev. 04/10) Application for a Search Warrant

FILED
FEB 22 2019
CLERK, U.S. DISTRICT COURT
RICHMOND, VA

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CALIFORNIA 94043

Case No. 3:19SW74 Under Seal

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 U.S.C. § 1951(a)	Hobbs Act Robbery

The application is based on these facts:

See Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Joahua P. Hylton, Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: February 22, 2019

/s/
David J. Novak
United States Magistrate Judge
Judge's signature

City and state: Richmond, Virginia

Honorable David J. Novak, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF: INFORMATION THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CALIFORNIA 94043

Case No. 3:19SW74

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Task Force Officer Joshua Hylton, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government copies of the information further described in Attachment B.

2. I am a duly appointed Task Force Officer with the Federal Bureau of Investigation (FBI) and have been so employed since December 2016. As such, I am an "investigative or law enforcement officer of the United States" within the meaning of § 2510(7) of Title 18, United States Code, that is, an officer of the United States empowered by law to conduct investigations and to make arrests for violations of federal law. I also have over seven

years of law enforcement experience as a police officer with the Chesterfield Police Department. I am currently assigned to the Richmond FBI's Central Virginia Violent Crimes Task Force where my duties include investigating bank robberies, extraterritorial offenses, armored car robberies, kidnappings, armed carjackings, and theft of government property. I have investigated numerous criminal violations and have obtained arrest and search warrants that have culminated in the successful prosecutions of their respective offenders. The crimes I investigate are violent in nature and usually involve two or more individuals. I am familiar with the methods violent offenders use to conduct their illegal activities, to include, but not limited to their communication methods, use of additional co-conspirators, and reoccurring method of operation

3. I have personally participated in the investigation of the offense discussed below. The facts and information contained in this affidavit are based upon my personal knowledge, or based on information obtained from federal law enforcement officers, and information obtained from interviews and analyses of reports. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1951(a), (robbery affecting commerce) have been committed by MICHAEL CARTER (M CARTER), JOSEPH CARTER (J CARTER), AND BRITTANY MATTHEWS (MATTHEWS). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further

described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." *See* 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

6. A cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

7. Google is an Internet company which, among other things, provides electronic communication services to subscribers. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience,

such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

8. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

9. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (*i.e.,* session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

10. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. Further, information maintained by the email provider can show how, where, and when the account was accessed or used. Based on my training and experience, I have learned that Google also maintains records that may reveal other Google accounts accessed from the same electronic device, such as the same computer or mobile device, including accounts that are linked by Hypertext Transfer Protocol (HTTP) cookies, which are small pieces of data sent from a website and stored in a user's Internet browser.

11. Google has developed an operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account and users are prompted to add a Google account when they first turn on a new Android device.

12. Based on my training and experience, I have learned that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. The company uses this information for location-based advertising and location-based search results. This information is derived from sources including GPS data, cell site/cell tower information, and Wi-Fi access points.

13. Location data can assist investigators in understanding the chronological and geographic context of the email account access and use relating to the crime under

investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email).

PROBABLE CAUSE

14. On January 5, 2019, at approximately 2230 hours, an unknown subject entered the Trolley Market, located at 1614 West Main Street, Richmond, Virginia. The subject approached victim, D.C., from behind, while brandishing a bladed weapon. The subject pressed the weapon against the side of D.C.'s neck and demanded United States currency from victim-clerk, H.V., who was standing near the store's register. H.V. complied with the subject's demands, giving him approximately $350.00 in United States currency belonging to the Trolley Market, before the subject fled from the business. The suspect was described as a white male wearing jeans, black mask, tan jacket, and black gloves wielding a black bladed weapon.

15. On January 6, 2019, at approximately 2317 hours, an unknown subject entered the Walgreens, located at 1798 North Parham Road, Henrico, Virginia. The subject approached victim-clerk, C.D., while brandishing a bladed weapon and demanded United States currency. The subject jumped the counter and approached C.D., who then opened the store's register. The subject removed approximately $300.00 in United States currency belonging to Walgreens and fled from the business. Surveillance video showed the suspect wearing a dark jacket with a gray/tan lining. The suspect was described as wearing a black mask and black gloves.

16. On January 7, 2019, at approximately 2115 hours, an unknown subject entered the BP gas station, located at 13623 Genito Road, Chesterfield, Virginia. The subject

approached victim-clerk, D.Y., while brandishing a bladed weapon, described as a large kitchen knife, and demanded United States currency. The subject jumped the counter and approached the register, while D.Y. ran from the business and called for emergency services. By the time law enforcement arrived on scene, approximately $300.00 in United States currency belonging to BP, was missing from the register. Surveillance video showed the suspect wearing a mask and dark colored jacket with gray/tan lining. The video also showed the suspect using what appeared to be a smaller blade to open the register. A gray or silver SUV was seen leaving the parking lot after the robbery.

17. On January 8, 2019, at approximately 2145 hours, an unknown subject entered the Spencer's convenience store, located at 4000 Kingsland Road, Chesterfield, Virginia. The subject approached victim-clerks, J.W. and C.H., while brandishing a bladed weapon and demanded United States currency. The subject jumped the counter and attempted to pry open the registers but was unsuccessful. The subject then ordered J.W. and C.H. to open the registers. The subject removed approximately $462.00 in United States currency belonging to Spencer's and fled from the business. Surveillance video showed the suspect wearing a mask, dark colored jacket with gray/tan lining, black zip-up hooded sweatshirt, and tan sheath with knife. The suspect was described as a white male wearing the sheath on his right side.

18. On January 9, 2019, at approximately 2256 hours, an unknown subject entered the FasMart convenience store, located at 1201 Westover Hills Boulevard, Richmond, Virginia. The subject approached victim-clerk, L.B., while brandishing a bladed weapon and demanded United States currency. The subject followed L.B. behind the counter and accessed the store's register. The subject obtained approximately $75.00 in United States currency belonging to

FasMart and fled from the business. Surveillance videos showed the suspect wearing a mask, black zip-up hooded sweatshirt, and a tan sheath with knife. The suspect was described as a white male wearing the sheath on his right side.

19. On January 11, 2019, at approximately 2146 hours, an unknown subject entered the Rite Aid pharmacy, located at 450 North Ridge Road, Henrico, Virginia. The subject approached victim-clerk, S.D., while brandishing a bladed weapon and demanded United States currency. S.D. complied with the subject's demands, giving him approximately $100.00 in United States currency belonging to Rite-Aid, before the subject fled from the business. The suspect was described as a white male wearing a black hooded sweatshirt, black jacket, mask covering the lower portion of his face, black gloves, and armed with a knife.

20. On January 11, 2019, at approximately 2152 hours, an unknown subject entered the CVS Pharmacy, located at 8901 Patterson Avenue, Henrico, Virginia. The subject approached victim-clerk, T.D., while brandishing a bladed weapon and demanded United States currency. The subject forced T.D. behind the counter at knifepoint to open the register. When T.D. opened the register, the subject took approximately $67.00 in United States currency belonging to CVS and fled from the business. Surveillance video showed a white male, wearing a mask, black zip-up hooded sweatshirt, and dark colored jacket with gray/tan lining.

21. On January 11, 2019, at approximately 2237 hours, an unknown subject entered the A-Plus gas station, located at 3101 Lauderdale Drive, Henrico, Virginia. The subject approached victim-clerk, B.W., while brandishing a bladed weapon and demanded United States currency. When B.W. opened the register, the subject took approximately $234.00 in United States currency belonging to A-Plus and fled from the business. Surveillance videos

show a white male wearing a mask, black zip-up hooded sweatshirt, and dark colored jacket with gray/tan lining.

22. On January 12, 2019, at approximately 2110 hours, an unknown subject entered the Lucky's convenience store, located at 14051 Steeplestone Drive, Chesterfield, Virginia. The subject approached victim-clerk, P.P., while brandishing a bladed weapon and demanded United States currency. P.P. complied with the unknown subject's demands, giving him approximately $250.00 in United States currency belonging to Lucky's, before the subject fled from the business. The suspect was described as a white male, wearing dark colored clothing, gloves, and a dark colored scarf covering the lower portion of the face, and brandishing a knife.

23. On January 13, 2019, at approximately 1916 hours, an unknown subject entered the Exxon gas station, located at 2708 Buford Road, Chesterfield, Virginia. The subject approached victim-clerk, C.B., while brandishing a bladed weapon and demanded United States currency. When C.B. opened the register, the subject took approximately $225.00 in United States currency belonging to Exxon and fled from the business. Surveillance videos show the suspect as a white male wearing a black mask, black zip-up hooded sweatshirt, and dark colored jacket with gray/tan lining.

24. On January 13, 2019, at approximately 1934 hours, an unknown subject entered the Shell gas station, located at 6232 Jahnke Road, Richmond, Virginia. The suspect was described as a younger white male wearing a mask, dark colored pants, jacket, and tan sheath on his right side. When addressed by clerk, A.B., the unknown subject quickly left the business on foot towards Brown Middle School, where law enforcement officers later located footprints and tire tracks in freshly fallen snow. Clerks stated that they recognized the suspect from

media releases of other similar robberies. M. CARTER subsequently admitted that he was the subject from this incident.

25. On January 13, 2019, at approximately 2250 hours, an unknown subject entered the Cary Street Mini Mart convenience store, located at 1317 West Cary Street, Richmond, Virginia. The subject approached victim-clerks, T.N. and E.H., while brandishing a bladed weapon and demanded United States currency. The subject threatened to hurt T.N. and E.H. if they called for help. While appearing to comply with the subject's demands, E.H. produced a firearm from under the counter. E.H. discharged the weapon in the direction of the subject, causing him to flee from the business. M CARTER subsequently admitted to having committed this attempted robbery.

26. On January 14, 2019, at approximately 0114 hours, an unknown subject entered the 7-Eleven convenience store, located at 5549 Belmont Road, Chesterfield, Virginia. The subject approached victim-clerk, R.P., while brandishing a bladed weapon and demanded United States currency. When R.P. opened the register, the unknown subject took approximately $190.00 in United States currency belonging to 7-Eleven and fled from the business. Upon the arrival of law enforcement officers, R.P. stated that R.P. recognized the suspect from media releases of other similar robberies.

27. On January 14, 2019, at approximately 2327 hours, an unknown subject entered the FasMart convenience store, located at 9492 Chamberlayne Road, Hanover, Virginia. The subject approached victim-clerk, G.M., while brandishing a bladed weapon and demanded United States currency. When G.M. opened the register, the subject took approximately $50.00 in United States currency belonging to FasMart. The subject also demanded scratch-off

Virginia Lottery tickets. G.M. complied, giving the subject one (1) Number 38 Extreme Millions ticket and eight (8) Virginia Lottery scratch-off tickets. The unique serial numbers for these tickets were provided to and subsequently flagged by the Virginia Lottery. Surveillance video shows the suspect as a white male, wearing a mask, black zip-up hooded sweatshirt, and dark colored jacket with gray/tan lining. M CARTER subsequently admitted to having committed this robbery.

28. On January 15, 2019 at 1002 hours, a subject, later identified as J CARTER, entered the Shell gas station, located at 1300 Anderson Highway, Powhatan, Virginia and attempted to redeem one of the Virginia Lottery scratch-off tickets from the robbery referenced in paragraph 27. J CARTER was unable to redeem the ticket because it had been flagged by the Virginia Lottery. Law enforcement responded to access surveillance video and interview employees C.S. and M.P. M.P. identified the individual who tried to redeem the stolen lottery ticket as JOSEPH CARTER, a regular customer of the gas station. Surveillance video showed J CARTER getting into the driver's seat of a gray Ford Escape as he left the gas station. Officers learned that J CARTER had a girlfriend named "BRITTNEY," who had asked the clerk about any job openings approximately two (2) years prior (later identified as BRITTNEY MATTHEWS). MATTHEWS provided the following phone number (804) 302-3491 to C.S. for return contact if a job opportunity became available.

29. While researching (804) 302-3491, investigators learned the number had been listed in a Powhatan County police report, dated August 16, 2014. In the report, MATTHEWS provided it as a contact number and JOSEPH CARTER was listed as a possible associate. In an additional report, dated October 22, 2018, originating from the Chesterfield County Police

Department, JOSEPH CARTER and brother, MICHAEL CARTER, provided (804) 302-3491 as their primary contact number. Additionally, MATTHEWS and J CARTER provided 1711 Anderson Highway (Apt C.), Powhatan, Virginia, as their place of residence.

30. On January 15, 2019, less than 20 minutes after J CARTER attempted to redeem one of the stolen lottery tickets, there was an attempt to redeem a second stolen lottery ticket. The subject entered the 7-Eleven, located at 13866 Village Place Dr., Midlothian, Virginia. The subject was unable to redeem the ticket because the ticket had been flagged by the Virginia Lottery. Law enforcement arrived on scene to access surveillance video and interview employee D.D. Surveillance video showed the white male getting into the front passenger's seat of a gray Ford Escape after his failed attempt to redeem the stolen lottery ticket. M CARTER subsequently admitted that he was the person who tried to redeem the stolen lottery ticket at 7-Eleven.

31. On January 15, 2019, at approximately 1930 hours, Henrico County Police detectives were provided a photograph from the Shell Gas Station security video of the gray Ford Escape J CARTER and unknown subject were observed in earlier that day. At approximately 2033 hours, detectives observed a gray Ford Escape, VA license plate UXP-3894, heading east on Midlothian Turnpike. The license plate was registered to BRITTNEY MATTHEWS, residing at 1711 Anderson Highway (Apt C.), Powhatan, Virginia. Detectives observed the Ford Escape exit westbound on Hull Street Road in Chesterfield, Virginia before losing sight of the vehicle in the area of Old Hundred Road.

32. At approximately 2103 hours, an unknown subject, entered the BP gas station, located at 13721 Hull Street Road, Chesterfield, Virginia (1.7 miles west of Old Hundred

Road). Upon entry, the subject opened an interior door separating customers from the employee work area behind the counter, and approached victim-clerk, A.P., while brandishing a bladed weapon and demanded United States currency. When A.P. opened the store registers, the subject took approximately $1,000.00 in United States currency belonging to the BP gas station and fled from the business. Surveillance videos showed the suspect was a white male, wearing a mask, black zip-up hooded sweatshirt, and dark colored jacket with gray/tan lining. M CARTER subsequently admitted to having committed this robbery.

33. At approximately 2113 hours, Chesterfield County detectives observed the gray Ford Escape, with VA license plate UXP-3894, heading east on Hull Street Road in Chesterfield, Virginia. Detectives continued following the vehicle until it arrived at a BP gas station, Steve's Food Mart, located at 5737 Hull Street Road, Richmond, Virginia. M CARTER subsequently admitted a drug transaction occurred at Steve's Food Mart. M CARTER admitted that using proceeds from the robbery, J CARTER purchased drugs from a known drug dealer.

34. After a few minutes, the vehicle left the parking lot of Steve's Food Mart and began travelling east on Hull street Road. Covert detectives continued following until the vehicle turned left on West Belt Boulevard and turned into the Ashton Square Apartments complex, located at 603 Westover Hills Boulevard, Richmond, Virginia. Investigators observed the SUV come to a stop near a unit located in the back-left portion of the property. The driver of the vehicle, later determined to be J CARTER, exited the SUV and walked to an apartment unit nearby. J CARTER returned minutes later and drove out of the complex towards Route 60. M CARTER subsequently admitted a drug transaction occurred at Ashton Square Apartments, with proceeds from the robbery, between JOSEPH CARTER and a known

drug dealer.

35. Law enforcement officers initiated a traffic stop in the area of the Chesterfield and Powhatan border on Midlothian Turnpike. As the SUV slowed to a stop, law enforcement officials observed an arm and hand extend from the passenger's side of the vehicle to throw an object from the window. Investigators located a pack of Marlboro Gold cigarettes, found in tall grass, approximately 8-10 feet from the passenger side of the vehicle. Inside the pack were tobacco products and a small plastic baggie containing white crystalized rocks. J CARTER subsequently claimed ownership of these items and identified the white crystalized rocks as "crack cocaine."

36. As detectives approached the car, the rear passenger, M CARTER, fled from the vehicle and ran into the woods north of the highway. With the assistance of an air unit utilizing thermal imaging cameras, K-9 units, and uniformed officers, M CARTER was taken into custody. K-9 handlers advised that as M CARTER was first fleeing from the vehicle, he was wearing a black hooded sweatshirt. By the time he was taken into custody, he was no longer wearing the black hooded sweatshirt. K-9 units re-ran M CARTER's track, at which point a black zip-up hooded sweatshirt was located, photographed, and collected. The black zip-up hooded sweatshirt was similar in appearance to the black zip-up hooded sweatshirt described from previous robberies.

37. The driver of the vehicle was identified as J CARTER and the front passenger of the vehicle was identified as MATTHEWS. In a search incident to arrest, a white HTC cell phone in a teal and pink case, $60 in U.S. currency, and cigarettes were found on MATTHEWS. In a search incident to arrest, a wallet, $534 in U.S. currency, and a black ZTE

cell phone with cracked screen were recovered from M CARTER.

38. The following items were in plain view within the Ford Escape: (A.) Wood/gold handled fixed blade knife, inside a tan leather sheath (back-passenger floorboard), (B.) A pair of form-fitting black material gloves (rear passenger seat), and (C.) black coat with tan colored lining. These items were similar in appearance to items visible in surveillance video and descriptions provided by victims of robberies referenced herein. The SUV was towed for processing and a black mask, similar in appearance and consistent with the description of the mask used in the robberies referenced above, was found within the pocket on the back side of the driver's seat.

39. After being advised of her rights pursuant to *Miranda,* MATTHEWS agreed to waive her rights. MATTHEWS claimed ownership of the white HTC cell phone found on her person. MATTHEWS stated that she and J CARTER are the primary users, but M CARTER has used it too. When asked to give an account of the evening, MATTHEWS denied any knowledge of the robbery and stated, "You need to talk to them" (indicating MICHAEL and JOSEPH CARTER).

40. After being advised of his rights pursuant to *Miranda*, J CARTER agreed to waive his rights. He admitted to using the white HTC cell phone and stated that he lived with MATTHEWS, and his brother M CARTER at 1711 Anderson Highway (Apt C.) in Powhatan, Virginia. While he denied knowledge of any additional robberies, J CARTER stated that he often drove M CARTER to locations for short periods of time. He stated that M CARTER would ask him to park at specific locations, so M CARTER could go and meet with friends to get money for illegal narcotics. When asked if he was able to recall any such instances, J

CARTER stated that he had recently driven M CARTER to Hanover County the previous evening and Carytown (Richmond) the evening prior to that. When shown a picture of his attempt to redeem a stolen lottery ticket at the Shell gas station in Powhatan, he said M CARTER had found them somewhere on the ground and had given J CARTER one to redeem. When questioned about purchasing illegal narcotics earlier that night, J CARTER denied any such activities, but admitted he owned the Marlboro cigarette box thrown from the vehicle, containing cigarettes and crack cocaine. Before being transported to the Chesterfield County Jail for processing, J CARTER admitted there were several small plastic baggies containing heroin and cocaine in his sock. Those items were then confiscated by law enforcement.

41. After being advised of his rights pursuant to *Miranda*, M CARTER agreed to waive his rights and admitted to his involvement in the following robberies: the BP gas station, located at 13721 Hull Street Road, Chesterfield, Virginia; FasMart convenience store, located at 9492 Chamberlayne Road, Hanover, Virginia; and the attempted robbery of Cary Street Mini Mart convenience store, located at 1317 West Cary Street, Richmond, Virginia.

42. M CARTER also admitted that he attempted to redeem the stolen lottery ticket at 7-Eleven, located at 13866 Village Place Drive, Midlothian, Virginia and that he was the person from the incident at the Shell gas station, located at 6232 Jahnke Road, Richmond, Virginia.

43. M CARTER stated that his brother, J CARTER, drove him to the businesses. M CARTER said he was the only one to enter the stores. When asked what motivated him to commit the robberies in question, M CARTER stated that he, J CARTER, and MATTHEWS were addicted to illegal narcotics, such as heroin and crack cocaine. M CARTER admitted that

the proceeds of the robberies were used to buy drugs just as they had done the night of the arrest. M CARTER stated that he uses both the white HTC cell phone and the black ZTE cell phone with cracked screen.

44. Based on my training and experience, I know that it is a common practice for persons, including person engaged in the criminal activity described here, to possess cellular telephones and keep them on their persons as they move throughout the day. Based on my training and experience, I also know that Google's Android operating system is one of the world's most common operating systems on cellular telephones. This leads me to believe that those involved in the robberies described herein, possessed a cellular telephone that may have had an Android operating system. Consequently, I believe that Google is in possession of information that could lead to the evidence of the perpetrators and evidence of these crimes.

45. The geographic region in Attachment A pertains to the same times and locations of the robberies, attempted robbery, and incidents described herein.

CONCLUSION

Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Joshua Hylton
Task Force Officer
Federal Bureau of Investigation

Reviewed and approved: Janet Jin Ah Lee, AUSA

SUBSCRIBED and SWORN before me this 22nd day of February, 2019

/S/
David J. Novak
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant is directed to Google LLC, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, and applies to: (1) GPS, Wi-Fi or Bluetooth sourced location history data generated from devices that reported a location within the geographical region bounded by the following latitudinal and longitudinal coordinates, dates, and times ("Initial Search Parameters"); and (2) identifying information for Google Accounts associated with the responsive location history data:

Location A.

Date: 01/05/2019

Time Period: From 10:00 pm to 10:45 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.547875, Longitude: -77.461431.



Location B.

Date: 01/06/2019

Time Period: From 10:45 pm to 11:15 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.611551, Longitude: -77.564477.



Location C.

Date: 01/07/2019

Time Period: From 8:45 pm to 9:30 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.449433, Longitude: -77.649779.



Location D.

Date: 01/08/2019

Time Period: From 9:15 pm to 10:00 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.404438, Longitude: -77.461392.



Location E.

Date: 01/09/2019

Time Period: From 10:30 pm – 11:15 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.519346, Longitude: 77.488477.



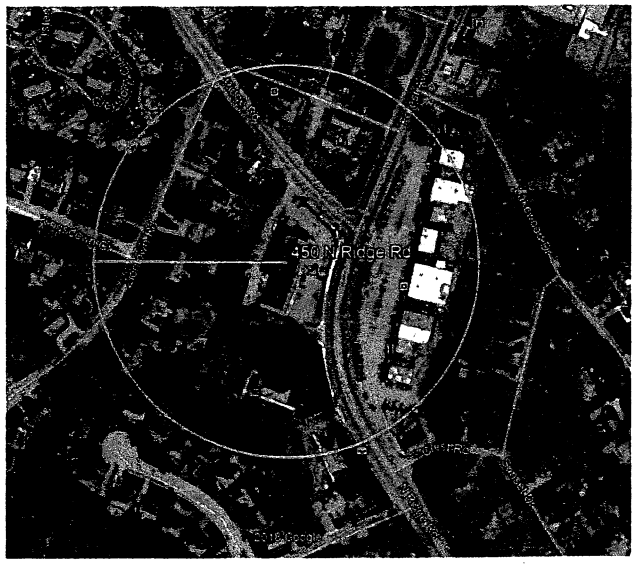
Location F.

Date: 01/11/2019

Time Period: From 9:15 pm to 10:00 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.582227, Longitude: -77.555586.



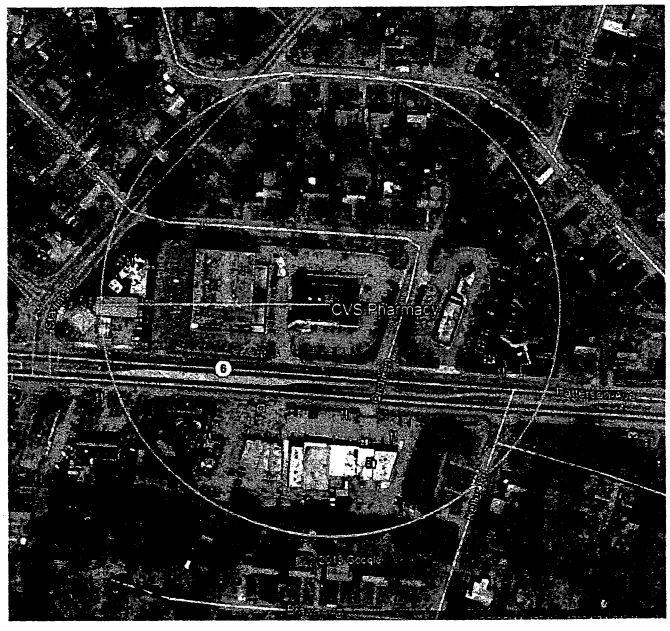
Location G.

Date: 01/11/2019

Time Period: From 9:15 pm to 10:00 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.595604, Longitude: -77.573692.



Location H.

Date: 1/11/2019

Time Period: From 10:00 pm to 10:45 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.638949, Longitude: -77.631822.



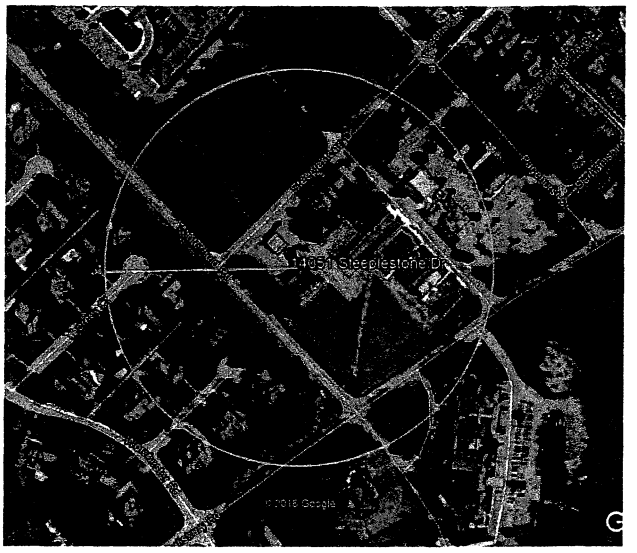
Location I.

Date: 01/12/2019

Time Period: From 8:00 pm to 9:30 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.525081, Longitude: -77.665754.



Location J.

Date: 01/13/2019

Time Period: From 6:45 pm to 7:35 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.534990, Longitude: -77.561975.



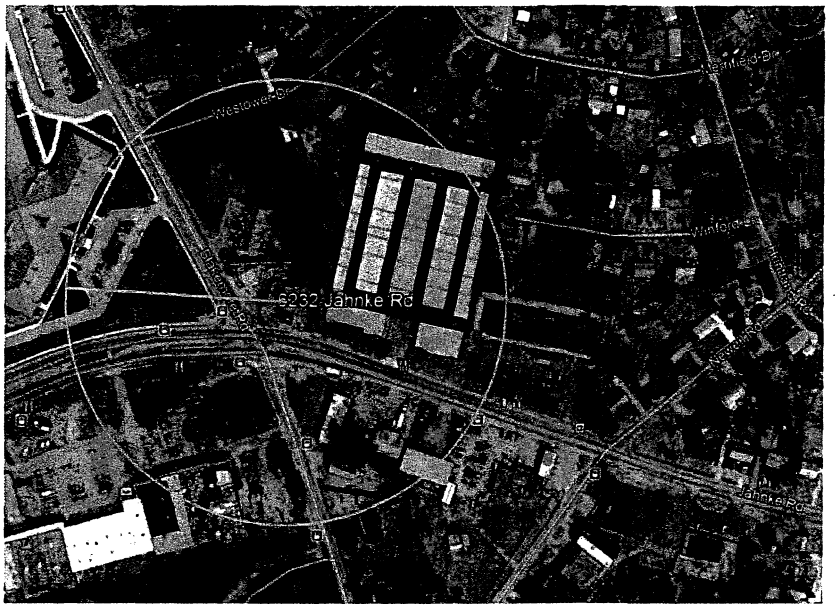
Location K.

Date: 01/13/2019

Time Period: From 7:00 pm to 7:50 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.520899, Longitude: -77.511673.



Location L.

Date: 01/13/2019

Time Period: From 10:20 pm to 11:05 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.545127, Longitude: -77.458523.



Location M.

Date: 01/13/2019

Time Period: From 12:45 pm – 1:30 am (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.459351, Longitude: -77.501554.



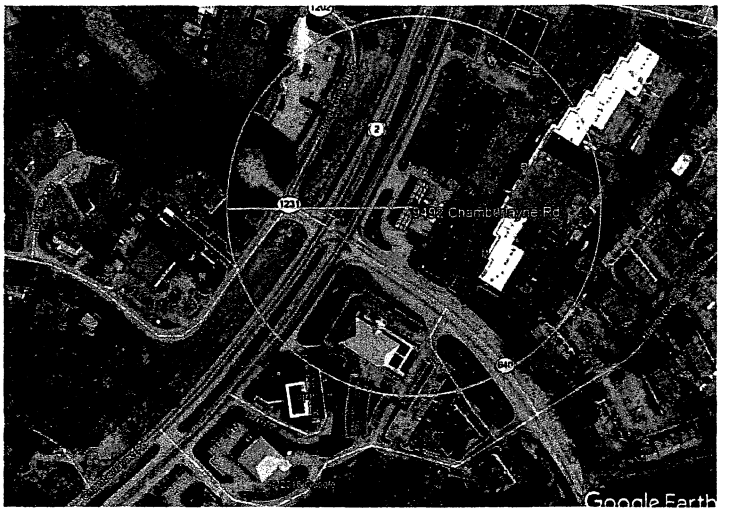
Location N.

Date: 01/14/2019

Time Period: From 11:05 pm – 11:55 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.658495, Longitude: -77.385696.



Location O.

Date: 01/15/2019

Time Period: From 8:30 pm – 9:15 pm (Eastern Standard Time)

Geographical area identified as

A radius of 150 meters around a latitude/longitude coordinate in the format Latitude: 37.406892, Longitude: -77.656733.



ATTACHMENT B

Items to Be Seized and Searched

I. Information to be disclosed by Google

Google shall provide responsive data (as described in Attachment A) pursuant to the following process:

1. Google shall query location history data based on the Initial Search Parameters (as described in Attachment A).

2. For each location point recorded within the Initial Search Parameters, Google shall produce anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the "Anonymized List").

3. Law enforcement shall review the Anonymized List to remove devices that are not relevant to the investigation, for example, devices that were not in the location for a sufficient period of time. If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the Time Period that fall outside of the Target Location. These contextual location coordinates may assist law enforcement in identifying devices that were located outside the Target Location, were not within the Target Location for a long enough period of time, were moving through the Target Location in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

4. For those device IDs identified as relevant pursuant to the process described

above, law enforcement may request that Google Provide identifying information, as defined in 18 U.S.C. § 2703(c)(2)(A)(B)(D) and (F), for the Google Account associated with each identified device ID. Additionally, for those device IDs identified as relevant pursuant to the process described above, law enforcement may request that Google Provide identifying information, as defined in 18 U.S.C. § 2703(c)(2)(C), for the Google Account associated with each identified device ID, for the period from January 1, 2019 to January 16, 2019.

USCA4 Appeal: 22-4489 Doc: 19-7 Filed: 01/20/2023 Pg: 86 of 362Total Pages:(1590 of 2164)

AFFIDAVIT FOR SEARCH WARRANT

Commonwealth of Virginia VA. CODE § 19.2-54

ALL INFORMATION SEALED

The undersigned Applicant states under oath:

RECEIVED & FILED
CHESTERFIELD CIRCUIT COURT
2019 JAN -8 AM 9:37
JEREMY S. HUGHES
CLERK OF COURT
TESTE:
CLERK/DEPUTY CLERK

1. A search is requested in relation to [ ] an offense substantially described as follows:
[ ] a person to be arrested for whom a warrant or process for arrest has been issued identified as follows:

Virginia State Code 18.2-58 Robbery

[ ] CONTINUED ON ATTACHED SHEET

2. The place, person or thing to be searched is described as follows:

See Attachment I

[ ] CONTINUED ON ATTACHED SHEET

3. The things or persons to be searched for are described as follows:

See Attachment II

[ ] CONTINUED ON ATTACHED SHEET

(OVER)

FORM DC-338 (MASTER, PAGE ONE OF TWO) 07/17

FILE NO. 42

AFFIDAVIT FOR SEARCH WARRANT

APPLICANT:

R.C. Humphries
NAME

Detective
TITLE (IF ANY)

PO BOX 148
ADDRESS

Chesterfield, VA 23832

Certified to Clerk of

CHESTERFIELD
CITY OR COUNTY Circuit Court

on 1-8-19
DATE

Detective
TITLE

SIGNATURE

Original Delivered [✓] in person [ ] by certified mail
[ ] by electronically transmitted facsimile
[ ] by use of filing/security procedures defined in the Uniform Electronic Transactions Act

to Clerk of CHESTERFIELD Circuit Court
CITY OR COUNTY WHERE EXECUTED

on 1-8-19
DATE

Detective
TITLE

SIGNATURE

J.A. 1534

USCA4 Appeal: 22-4489 Doc: 19-7 Filed: 01/20/2023 Pg: 87 of 362Total Pages:(1591 of 2164)

4. The material facts constituting probable cause that the search should be made are:

See Attachment III

ALL INFORMATION SEALED

5. The object, thing or person searched for [X] constitutes evidence of the commission of such offense [ ] is the person to be arrested for whom a warrant or process for arrest has been issued.

6. [X] I have personal knowledge of the facts set forth in this affidavit AND/OR

[ ] I was advised of the facts set forth in this affidavit, in whole or in part, by one or more other person(s). The credibility of the person(s) providing this information to me and/or the reliability of the information provided may be determined from the following facts:

See Attachment IV

The statements above are true and accurate to the best of my knowledge and belief.

Detective
TITLE OF APPLICANT

RC Humphries
APPLICANT

Subscribed and sworn to before me this day.

1/24/19 1057
DATE AND TIME

[ ] CLERK [ ] MAGISTRATE [X] JUDGE

E.C Rockwell - III

FORM DC-338 (MASTER, PAGE TWO OF TWO) 07/17

ALL INFORMATION SEALED

42

ATTACHMENT I
PERSON, PLACE, OR THING TO BE SEARCHED:

This data is maintained on computer servers that are stored at premises controlled by Google Inc., a company that accepts service of legal process at 1600 Amphitheater Parkway, Mountain View, California 94043.

Your affiant knows that Google Inc. maintains certain records during the normal course of business and when properly served with a legal request, Google Inc. will provide Law Enforcement with the said records. Your affiant also knows that these electronic records will further support the ongoing criminal investigation. Your affiant believes that the records requested are actually or constructively possessed by a foreign corporation, Google Inc. that provides electronic communication service or remote computing service within the Commonwealth of Virginia.

Your affiant knows that section 19.2-70.3 of the Code of Virginia states that a provider of electronic communication service or remote computing service, which includes a foreign corporation that provides such services, shall disclose certain business records pertaining to their customers, excluding the contents of electronic communications and real-time location data, to an investigative or law-enforcement officer if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation. This warrant shall be properly served on the entity named above in accordance with 19.2-70.3 of the code of Virginia.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider, Google Inc. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in ATTACHMENT II.

ALL INFORMATION SEALED

ATTACHMENT II
THE THINGS OR PERSONS TO BE SEARCHED FOR:

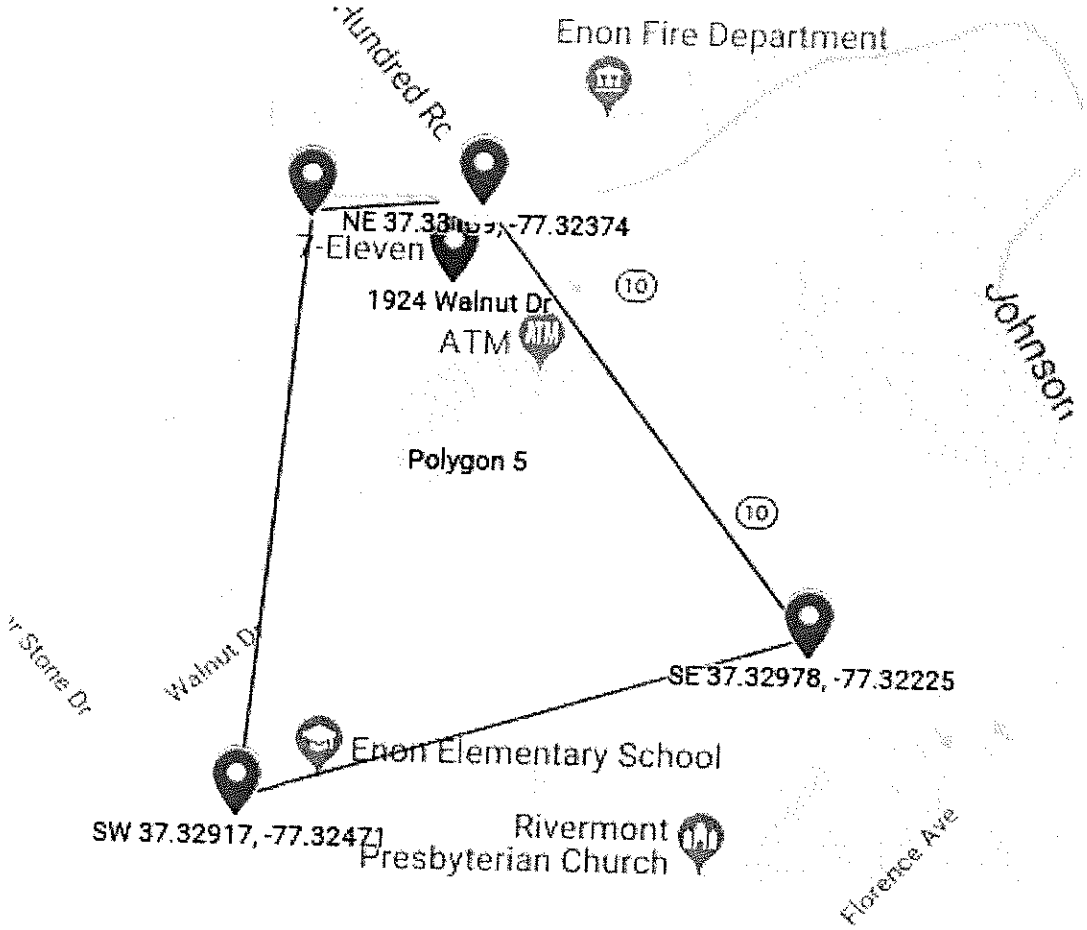
The facts and circumstances outlined in this affidavit brought on by your Affiant suggest that there is probable cause to believe evidence of the commission of the crime of **Robbery**, a violation of **Virginia code 18.2-58** (hereinafter "Subject"), may be found within computer servers maintained or controlled by Google, Inc. or Google Payment Corp. Such accounts are described further in ATTACHMENT II (hereinafter "the Accounts") stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043. The following material is sought for the time period of **October 7th, 2016 @ 1622hrs EST – October 8th, 2016 @ 1222hrs EST.**

1. For each type of Google account that is associated with a device that was inside the geographical area described further in ATTACHMENT II, **during the time frame listed above,** Google will provide **"anonymized information"** regarding the Accounts that are associated with a device that was inside the described geographical area during the time frame described above. This **"anonymized information"** will include a numerical identifier for the account, the type of account, time stamped location coordinates and the data source that this information came from if available. The information initially provided by Google will not contain any further content or information identifying the user of a particular device or account.
2. Law enforcement officers will review this **"anonymized information"** provided by Google, Inc. in an effort to narrow down the list of accounts associated with devices identified in the **"anonymized information".** Law enforcement officers will attempt to narrow down the list by reviewing the time stamped location coordinates for each account and comparing that against the known time and location information that is specific to this crime.
3. Law enforcement officers will return a list that they have attempted to narrow down. This list will still be identified by the "**anonymized information**" described above. After this review by Law Enforcement and upon request, Google, Inc. shall produce "contextual data points with points of travel outside of the geographical area" described further in ATTACHMENT II of this Application for Search Warrant. The time frame will be expanded for this production of "contextual data points with points of travel outside of the geographical area" for 30 minutes before AND 30 minutes after the initial search time periods. This expanded time frame will be from **October 7th, 2016 @ 1622hrs EST – October 8th, 2016 @ 1222hrs EST + & - 30 MINUTES**. Google Inc. shall provide this additional information to Law Enforcement for review.
4. Law Enforcement officers will review this additional information along with the **"anonymized information"** and will attempt to narrow down the list by comparing this additional information regarding travel and time against the known time and location information that is specific to this crime.
5. After review and upon request by Law Enforcement, Google Inc. shall provide identifying account information / CSI for the account/s requested by Law Enforcement. This identifying account information / CSI shall include all of the following that are available: user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used to set up the account, verify the account or to receive assistance with the account, and Google Voice phone numbers associated with the account.

ALL INFORMATION SEALED

ATTACHMENT II
THE THINGS OR PERSONS TO BE SEARCHED FOR (CONTINUED):

This search warrant applies to the Google Accounts associated with devices that were located inside the following geographical areas: NW Corner: **37.33134, -77.32448**, NE Corner: **37.33139, -77.32374**, SW Corner: **37.32917, -77.32471**, SE Corner: **37.32978, -77.32225** During the following time frame: **October 7th, 2016 @ 1622hrs EST – October 8th, 2016 @ 1222hrs EST.**



ALL INFORMATION SEALED

ATTACHMENT III

MATERIAL FACTS CONSTITUTING PROBABLE CAUSE:

The Affiant swears to the following facts to establish probable cause for the issuance of a search warrant:

On October 8th, 2016 at approximately 0222hrs (EST) a black male entered the 7-11 Convenience Store located at 1924 Walnut Drive in Chesterfield County, Virginia. The black male had his face partially covered and displaying a revolver. The suspect approached Dejon Fitch, a store employee and pointed the firearm at him demanding money. Fitch opened a cash register and the suspect removed cash. The suspect demanded Fitch open the other register which he did, it was empty. The suspect ultimately fled the store on foot with the stolen currency. The incident was captured by the stores video surveillance system.

This applicant knows a cellular telephone or mobile telephone is a handheld wireless device primarily used for voice, text, and data communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called "cells" or "cell sites," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") or other technology for determining a more precise location of the device.

This applicant also knows that Google is a company, which, among other things, provides electronic communication services to subscribers, including email services. Google allows subscribers to obtain email accounts at the domain name gmail.com and/or google.com. Subscribers obtain an account by registering with Google. A subscriber using the Provider's services can access his or her email account from any computer/device connected to the Internet.

This applicant knows that Google has also developed a proprietary operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

Based on this applicant's training and experience, this applicant knows that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled. The company uses this information for location-based advertising and location-based search results and stored such data in perpetuity unless it is manually deleted by the user. This location information is derived from GPS data, cell site/cell tower information, Bluetooth connections, and Wi-Fi access points.

ALL INFORMATION SEALED

ATTACHMENT III
MATERIAL FACTS CONSTITUTING PROBABLE CAUSE (CONTINUED):

This applicant knows that location data can assist investigators in forming a fuller geospatial understanding and timeline related to a specific criminal investigation; and may tend to identify potential witnesses and/or suspects. Such information can also aid investigators in possibly inculpating or exculpating persons of interest.

Additionally, location information can be digitally integrated into image, video, or other computer files associated with a Google account and can indicate the geographic location of the accounts user at a particular date and time (e.g., digital cameras, including on cellular telephones, frequently store GPS coordinates indicating where a photo was taken in the "metadata" of an image file).

Your affiant knows that in a Pew Research Center study released in October of 2015, it was determined that 92% of American adults own a cellular phone with 56% being smartphones. Pew Research Center is located at 1615 L St. NW, Suite 800 Washington, DC 20036 and conduct public opinion polling, demographic research, content analysis and other data-driven social science research. Because of this, your Affiant believes that there is probable cause to believe that the offender(s) in the **Robbery** would have had a mobile device on their person or within close proximity to them.

ALL INFORMATION SEALED

ATTACHMENT IV
CREDIBILITY OF PERSON(S) PROVIDING INFORMATION:

I, Detective, R.C. Humphries #938, hereafter referred to as your Affiant, do hereby swear and affirm that the information contained herein is true and correct to the best of my knowledge and belief. Your affiant has been a sworn Law Enforcement Officer in Chesterfield County, Virginia since 1993. Your affiant is currently assigned to the Criminal Investigations Division, Unsolved Major Investigations Group. Your affiant has served as a patrol officer, field training officer and detective. Your affiant has investigated multiple crimes that have been successfully prosecuted to include: possession/distribution of narcotics, assaults, malicious wounding, robberies, and homicides. Your affiant has completed specialized training in the topics of interviews, identification and collection of evidence, topics pertaining to law, search and seizure, criminal, robbery, death investigations, and property crimes. Investigations conducted by your affiant have been prosecuted successfully in the General District Courts, Juvenile and Domestic Relations Courts, and Circuit Courts of Chesterfield County. This affidavit is being submitted for the limited purpose of obtaining a search warrant for the premises described below, it is not intended to include each and every fact and matter observed by me or known to the government. Therefore, your affiant has set forth only those facts necessary to support probable cause for this application.

Your affiant is requesting a search warrant in relation to violation of Virginia State Code Section 18.2-32 in violation code of Virginia.

USCA4 Appeal: 22-4489 Doc: 19-7 Filed: 01/20/2023 Pg: 94 of 362 Total Pages:(1598 of 2164)

AFFIDAVIT FOR SEARCH WARRANT

Commonwealth of Virginia VA. CODE § 19.2-54

ALL INFORMATION SEALED

The undersigned Applicant states under oath:

1. A search is requested in relation to [X] an offense substantially described as follows:
   [ ] a person to be arrested for whom a warrant or process for arrest has been issued identified as follows:

   Virginia State Code 18.2-58 Robbery

[ ] CONTINUED ON ATTACHED SHEET

2. The place, person or thing to be searched is described as follows:

   See Attachment I.

[ ] CONTINUED ON ATTACHED SHEET

3. The things or persons to be searched for are described as follows:

   See Attachment II.

FILED IN THE CLERK'S OFFICE OF THE CIRCUIT COURT OF CHESTERFIELD COUNTY, VIRGINIA
2019 APR 11 AM 10:
CLAIRE G. HUGHES CLERK OF COURT
BY: DEPUTY CLERK

[ ] CONTINUED ON ATTACHED SHEET

(OVER)

FORM DC-338 (MASTER, PAGE ONE OF TWO) 07/17

FILE NO. 472 ✓

AFFIDAVIT FOR SEARCH WARRANT

APPLICANT:

J.P. Hylton
NAME

Master Detective
TITLE (IF ANY)

PO BOX 148
ADDRESS

Chesterfield, VA 23832

Certified to Clerk of Chesterfield Circuit Court
CITY OR COUNTY

on April 11, 2019
DATE

Detective
TITLE

SIGNATURE

Original Delivered [X] in person [ ] by certified mail
[ ] by electronically transmitted facsimile
[ ] by use of filing/security procedures defined in the Uniform Electronic Transactions Act

to Clerk of Chesterfield Circuit Court
CITY OR COUNTY WHERE EXECUTED

on April 11, 2019
DATE

Detective
TITLE

SIGNATURE

J.A. 1542

ALL INFORMATION SEALED

4. The material facts constituting probable cause that the search should be made are:

See Attachment III.

5. The object, thing or person searched for [X] constitutes evidence of the commission of such offense [ ] is the person to be arrested for whom a warrant or process for arrest has been issued.

6. [X] I have personal knowledge of the facts set forth in this affidavit AND/OR

[ ] I was advised of the facts set forth in this affidavit, in whole or in part, by one or more other person(s). The credibility of the person(s) providing this information to me and/or the reliability of the information provided may be determined from the following facts:

See Attachment IV.

2019 APR 11 AM 10:55
CLERK OF COURT
DEPUTY CLERK

The statements above are true and accurate to the best of my knowledge and belief.

Master Detective
TITLE OF APPLICANT

APPLICANT

Subscribed and sworn to before me this day.

4/4/19 3:35 p.m.
DATE AND TIME

[ ] CLERK [ ] MAGISTRATE [ ] JUDGE

FORM DC-338 (MASTER, PAGE TWO OF TWO) 07/17

J.A. 1543
Filed: 01/20/2023 Pg: 95 of 362 Total Pages:(1599 of 2164)
USCA4 Appeal: 22-4489 Doc: 19-7

ALL INFORMATION SEALED

ATTACHMENT I.
PERSON, PLACE, OR THING TO BE SEARCHED:

This data is maintained on computer servers that are stored at premises controlled by Google Inc., a company that accepts service of legal process at 1600 Amphitheater Parkway, Mountain View, California 94043.

Your affiant knows that Google Inc. maintains certain records during the normal course of business and when properly served with a legal request, Google Inc. will provide Law Enforcement with the said records. Your affiant also knows that these electronic records will further support the ongoing criminal investigation. Your affiant believes that the records requested are actually or constructively possessed by a foreign corporation, Google Inc. that provides electronic communication service or remote computing service within the Commonwealth of Virginia.

Your affiant knows that section 19.2-70.3 of the Code of Virginia states that a provider of electronic communication service or remote computing service, which includes a foreign corporation that provides such services, shall disclose certain business records pertaining to their customers, excluding the contents of electronic communications and real-time location data, to an investigative or law-enforcement officer if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation. This warrant shall be properly served on the entity named above in accordance with 19.2-70.3 of the code of Virginia.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider, Google Inc. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in ATTACHMENT II.

2019 APR 11 AM 10:55

ALL INFORMATION SEALED

ATTACHMENT I.
PERSON, PLACE, OR THING TO BE SEARCHED:

This data is maintained on computer servers that are stored at premises controlled by Google Inc., a company that accepts service of legal process at 1600 Amphitheater Parkway, Mountain View, California 94043.

Your affiant knows that Google Inc. maintains certain records during the normal course of business and when properly served with a legal request, Google Inc. will provide Law Enforcement with the said records. Your affiant also knows that these electronic records will further support the ongoing criminal investigation. Your affiant believes that the records requested are actually or constructively possessed by a foreign corporation, Google Inc. that provides electronic communication service or remote computing service within the Commonwealth of Virginia.

Your affiant knows that section 19.2-70.3 of the Code of Virginia states that a provider of electronic communication service or remote computing service, which includes a foreign corporation that provides such services, shall disclose certain business records pertaining to their customers, excluding the contents of electronic communications and real-time location data, to an investigative or law-enforcement officer if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation. This warrant shall be properly served on the entity named above in accordance with 19.2-70.3 of the code of Virginia.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider, Google Inc. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in ATTACHMENT II.

ALL INFORMATION SEALED

ATTACHMENT II.
THE THINGS OR PERSONS TO BE SEARCHED FOR:

The facts and circumstances outlined in this affidavit brought on by your Affiant suggest that there is probable cause to believe evidence of the commission of the crime of **Robbery**, a violation of **Virginia code 18.2-58** (hereinafter "Subject"), may be found within computer servers maintained or controlled by Google, Inc. or Google Payment Corp. Such accounts are described further in ATTACHMENT II. (hereinafter "the Accounts") stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043. The following material is sought for the time periods as listed below:

- **Date/Time: 07/07/2018 at 2130 hours (EST) – 07/08/2018 at 0000 hours (EST)**

1. For each type of Google account that is associated with a device that was inside the geographical area described further in ATTACHMENT II., **during the time frame listed above,** Google will provide **"anonymized information"** regarding the Accounts that are associated with a device that was inside the described geographical area during the time frame described above. This **"anonymized information"** will include a numerical identifier for the account, the type of account, time stamped location coordinates and the data source that this information came from if available. The information initially provided by Google will not contain any further content or information identifying the user of a particular device or account.

2. Law enforcement officers will review this **"anonymized information"** provided by Google, Inc. in an effort to narrow down the list of accounts associated with devices identified in the **"anonymized information."** Law enforcement officers will attempt to narrow down the list by reviewing the time stamped location coordinates for each account and comparing that against the known time and location information that is specific to this crime.

3. Law enforcement officers will return a list that they have attempted to narrow down. This list will still be identified by the "**anonymized information**" described above. After this review by Law Enforcement and upon request, Google, Inc. shall produce "contextual data points with points of travel outside of the geographical area" described further in ATTACHMENT II. of this Application for Search Warrant. The time frame will be expanded for this production of "contextual data points with points of travel outside of the geographical area" for 30 minutes before AND 30 minutes after the initial search time periods. This expanded time frame will be as listed below (Google Inc. shall provide this additional information to Law Enforcement for review):

- **1st Date/Time: 07/07/2018 at 2130 hours – 07/08/2018 at 0000 hours (+/- 30 Minutes) Eastern Standard Time (EST)**

4. Law Enforcement officers will review this additional information along with the **"anonymized information"** and will attempt to narrow down the list by comparing this

ALL INFORMATION SEALED

additional information regarding travel and time against the known time and location information that is specific to this crime.

5. After review and upon request by Law Enforcement, Google Inc. shall provide identifying account information/CSI for the accounts requested by Law Enforcement. This identifying account information/CSI shall include all of the following that are available: user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used to set up the account, verify the account or to receive assistance with the account, and Google Voice phone numbers associated with the account.

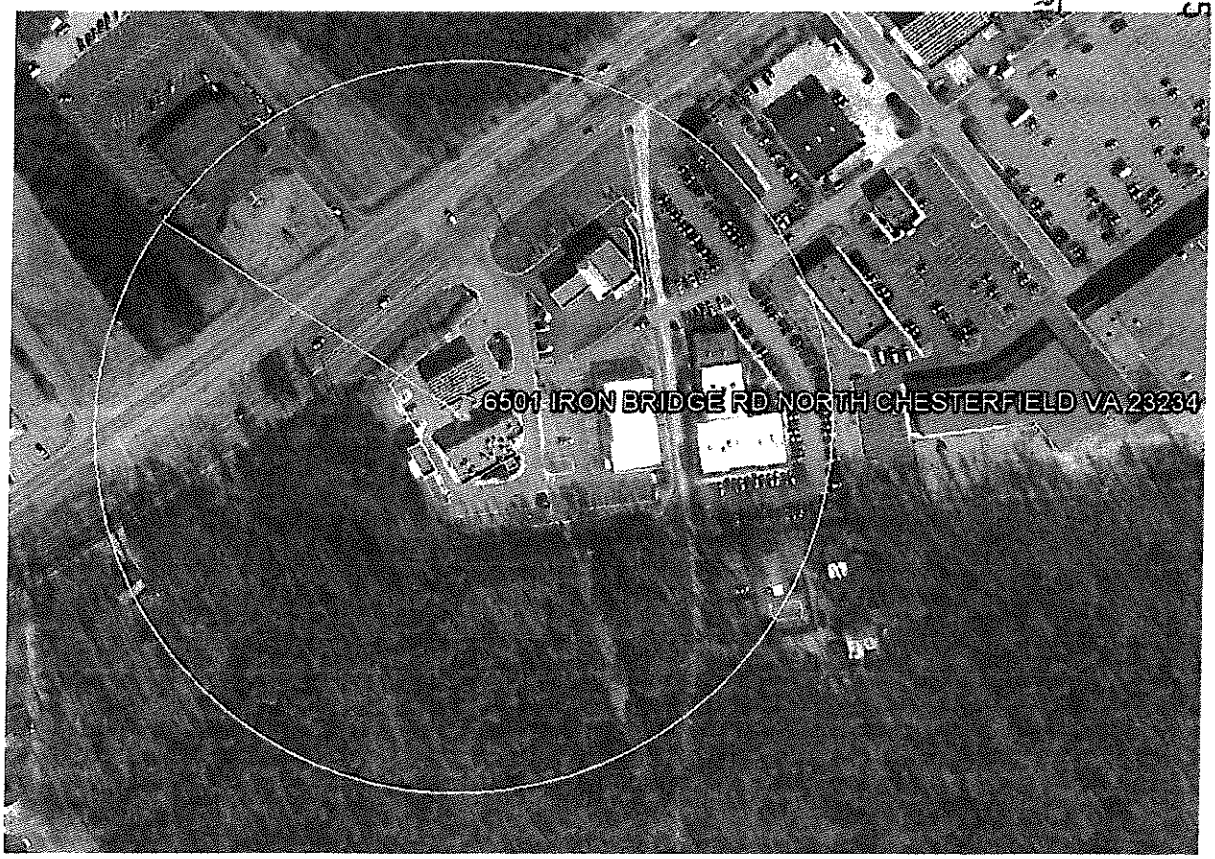
This search warrant applies to the Google Accounts associated with devices that were located inside the geographical regions bounded by the following latitudinal and longitudinal coordinates, dates, and times:

Location A.

Date/Time: **07/07/2018 at 2130 hours (EST) – 07/08/2018 at 0000 hours (EST)**

Geographical Area: Radius of 150 meters around a latitude/longitude coordinate. **Latitude: 37.426567, Longitude: -77.494904**

2019 APR 11 A 10:55
CLERK OF COURT



ALL INFORMATION SEALED

ATTACHMENT III.

MATERIAL FACTS CONSTITUTING PROBABLE CAUSE:

The Affiant swears to the following facts to establish probable cause for the issuance of a search warrant:

On July 7th, 2018 at approximately 2310 hours, an unknown subject (UNSUB) entered the 7-Eleven gas station, located at 6501 Iron Bridge Road, Chesterfield, Virginia 23832. The UNSUB approached victim-clerk, T.S., while brandishing a black handgun and demanding United States currency from the store's register. T.S. complied, giving the UNSUB approximately $200.00 in United States currency belonging to 7-Eleven. After acquiring said funds, the UNSUB fled the business on foot and was further described as a black male, medium build, wearing a red/orange hooded sweatshirt, khaki pants, mask, blue latex gloves, and wielding a black handgun.

Following review of surveillance video, a suspicious vehicle was observed in the business' parking lot minutes prior to the store being robbed. Occupants of said vehicle entered the business separately at various times, but later left in the same sedan. After leaving the 7-Eleven parking lot, the vehicle was observed parked near Iron Bridge Road for several minutes (just prior to the UNSUB walking towards 7-Eleven). In the undersigned's experience, this type of behavior is normally observed when two or more parties are casing a business before a robbery.

Your affiant finds it necessary and prudent to request that Google provide Geo Fencing data in order to assist with the investigation. In the undersigned's training and experience, when people act in concert with one another to commit a crime, they frequently utilize cellular telephones and other such electronic devices, to communicate with each other through WiFi, Bluetooth, GPS, voice calls, text messages, social media accounts, applications, emails, and/or cell towers in the area of the victim-business, located at 6501 Iron Bridge Road, Chesterfield, Virginia 23832. Furthermore, the requested data/information would have been captured by Google during the requested time.

This applicant knows a cellular telephone or mobile telephone is a handheld wireless device primarily used for voice, text, and data communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called "cells" or "cell sites," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") or other technology for determining a more precise location of the device.

This applicant also knows that Google is a company, which, among other things, provides electronic communication services to subscribers, including email services. Google allows subscribers to obtain email accounts at the domain name gmail.com and/or google.com. Subscribers obtain an account by registering with Google. A subscriber using the Provider's services can access his or her email account from any computer/device connected to the Internet.

ALL INFORMATION SEALED

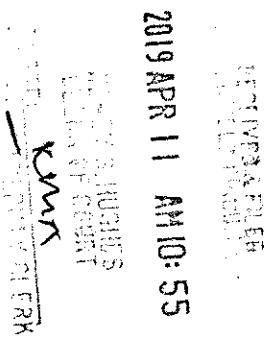
This applicant knows that Google has also developed a proprietary operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

Based on this applicant's training and experience, this applicant knows that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled. The company uses this information for location-based advertising and location-based search results and stored such data in perpetuity unless it is manually deleted by the user. This location information is derived from GPS data, cell site/cell tower information, Bluetooth connections, and Wi-Fi access points.

This applicant knows that location data can assist investigators in forming a fuller geospatial understanding and timeline related to a specific criminal investigation; and may tend to identify potential witnesses and/or suspects. Such information can also aid investigators in possibly inculpating or exculpating persons of interest.

Additionally, location information can be digitally integrated into image, video, or other computer files associated with a Google account and can indicate the geographic location of the account's user at a particular date and time (e.g., digital cameras, including on cellular telephones, frequently store GPS coordinates indicating where a photo was taken in the "metadata" of an image file).

Your affiant knows that in the September 2013 Pew Research Center study, it was determined that 91% of American adults own a cellular phone with 56% being smartphones. Pew Research Center is located at 1615 L St. NW, Suite 800 Washington, DC 20036 and conduct public opinion polling, demographic research, content analysis and other data-driven social science research. Because of this, your Affiant believes that there is probable cause to believe that the offender(s) in the robbery would have had a mobile device on their person or within close proximity to them.

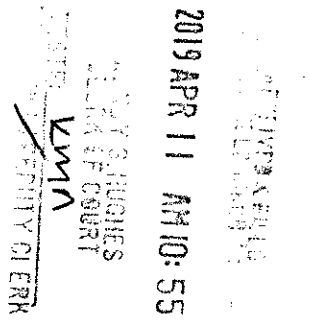


ALL INFORMATION SEALED

ATTACHMENT IV.
CREDIBILITY OF PERSON(S) PROVIDING INFORMATION:

I, Detective, J.P. Hylton, do hereby swear and affirm that the information contained herein is true and correct to the best of my knowledge and belief. Your affiant has over seven years of law enforcement experience stemming from employment as a police officer with the Chesterfield County Police Department. The undersigned is a duly appointed Task Force Officer with the Federal Bureau of Investigation (FBI). Your affiant is assigned to the Richmond FBI's Central Virginia Violent Crimes Task Force, where his duties include investigating extraterritorial offenses, commercial and bank robberies, murder, kidnappings, serial offenses, armed carjackings, and theft of government property. The undersigned has investigated numerous criminal violations and obtained multiple arrest and search warrants, culminating in the successful prosecution of their respective offenders. Your affiant is familiar with the methods violent offenders use to conduct their illegal activities, to include their communication techniques, utilization of electronic devices for planning/execution, use of additional co-conspirators, and reoccurring method of operation (MO). This affidavit is being submitted for the limited purpose of obtaining a search warrant for the premises described herein, it is not intended to include each and every fact and matter observed by the undersigned or known to the government. Therefore, your affiant has set forth only those facts necessary to support probable cause for this application.

Your affiant is requesting a search warrant in relation to violation of Virginia State Code Section 18.2-58 Robbery.



ATTACHMENT A

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA v. OKELLO T. CHATRIE, *Defendant*.	Case No. 3:19-cr-00130-MHL

DECLARATION OF MARLO MCGRIFF

I, Marlo McGriff, respectfully submit this declaration in regard to the above-captioned matter. I make this declaration based on my knowledge of the facts stated herein.

1. I am a Location History Product Manager at Google, where my responsibilities include the Location History product. I joined Google in 2011 and have been in my current role since 2016.

2. I lead the cross-functional Location History team and am the overall Location History lead, setting the near-term goals and long-term strategy for the product.

I. Google Location History

3. Some Google services require a user to have a Google account before she can use the service at all, like Gmail. Other services do not require a user to have an account, but offer additional functionality that is only available to Google account holders, like Maps and Search.

4. Google Location History ("LH") is a service that Google account holders may choose to use to keep track of locations they have visited while in possession of their compatible

mobile devices. LH is not available to users who do not have a Google account. Users must explicitly opt in to the service.[1]

5. Google users can visualize their LH data through the "Timeline" feature of Google Maps, which operates as a journal that Google users can choose to use to create, edit, and store a record of their movements and travels. The Timeline feature processes the user's LH data to infer semantic location information such as place visits (*e.g.*, visit to a ski resort), activities (*e.g.*, driving), and paths between place visits (*e.g.*, driving from hotel to ski resort), which is then displayed to the user in her Timeline. LH and the Timeline feature thus allow a user to see where she has traveled with her device and when over a given period.

6. Users who opt into and use LH can access other benefits on their Google devices or applications as well. For instance, they can obtain personalized maps or recommendations based on places they have visited, get help finding their phones, and receive real-time traffic updates about their commutes.

7. For Google LH to function and save information about a user's location, the user must take several steps—some tied to her mobile device, some tied to her Google account.[2] First, the user must ensure that the device-location setting on her mobile device is turned on. When the device-location setting is activated, the mobile device automatically detects its own location, which the device ascertains based on GPS and Bluetooth signals, Wi-Fi connections, and cellular networks. Android users can also tailor their devices' location-reporting settings, controlling which sources of information (*e.g.*, GPS, cellular, or Wi-Fi) the device may use to

---

[1] *See* Google, *Manage Your Location History*, https://support.google.com/accounts/answer/3118687?hl=en (visited Feb. 27, 2020).

[2] *See generally id.*; Google Privacy & Terms, *How is location saved in my Google Account*?, https://policies.google.com/technologies/location-data#how-save (visited Feb. 27, 2020).

determine location, and which applications can access location data. On iOS devices, the user must further configure her mobile device to share location information by granting the required device-level application location permission.

8. However, merely taking the steps described above—steps that are tied to a mobile device—does not on its own enable LH for a user's account. Google does not save LH information about where a particular mobile device has been to a user's account—even when the device-location feature is turned on and (for iOS) the required device-level application location permissions have been granted—unless the user has also taken additional specific steps tied to her account.

9. For one, the user must opt into LH in her account settings and enable "Location Reporting"—a subsetting within LH—for each particular device on which she wants to use LH. And to actually record and save LH data, the user must then sign into her Google account on her device and travel with that device. A single Google account can be associated with multiple devices, and the "Location Reporting" feature within LH allows users to select the specific devices on which they wish to enable LH.

10. In sum, LH functions and saves a record of the user's travels only when the user opts into LH as a setting on her Google account, enables the "Location Reporting" feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it.

11. When a user takes the above-mentioned steps, the resulting data is communicated to Google for processing and storage. Google stores this data in a database internally referred to as "Sensorvault." Only LH information is stored in Sensorvault.

12. LH information may be considerably more precise than other kinds of location data, including cell-site location information ("CSLI"). That is because, as a technological matter, a mobile device's location-reporting feature can use multiple inputs in estimating the device's location. Those inputs could include GPS signals (*i.e.*, radio waves detected by a receiver in the mobile device from orbiting geolocation satellites) or signals from nearby Wi-Fi networks, Bluetooth beacons, or cell towers. Combined, these inputs (when the user enables them) can be capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI. For example, I understand that when a strong GPS signal is available, a device's location can be estimated within approximately twenty meters or less.

13. In 2019, the majority of Google users worldwide did not have LH enabled on their account. While a more precise percentage is difficult to calculate in part due to fluctuating numbers of users, in 2019, roughly one-third of active Google users (i.e., numerous tens of millions of Google users) had LH enabled on their accounts.

14. Depending on a user's ads personalization setting, Google may use the semantic location information described in Paragraph 5 above (*e.g.*, place visits) that the Timeline feature infers from LH to show relevant ads to the user. For example, a user who regularly frequents ski resorts may later see an ad for ski equipment when watching a video on YouTube. Additionally, Google may also use the semantic location information that the Timeline feature infers from LH in an anonymized and aggregated manner to help advertisers measure how often an online ad campaign helps drive traffic to physical stores or properties. Google does not share LH or any other information identifying individual users with advertisers.[3] Additionally, at all times

[3] *See* Google Privacy & Terms, *How is location used to show ads?*, https://policies.google.com/technologies/location-data#show-ads (visited Feb. 27, 2020).

relevant to this warrant, Google has not shared identified LH data with third parties except through legal process and has not monetized identified LH data.

15. Critically, as described in Google's Privacy Policy at https://policies.google.com/technologies/retention, a user remains in control of her LH data through her Timeline. She can review, edit, or delete her Timeline at will. By deleting Timeline entries, a user also deletes the underlying LH information. As such, the user could decide to keep LH information only for certain dates; she could delete all LH information except those associated with certain Timeline entries; she could instruct Google to automatically delete all LH information after a set period; or she could keep all LH information for future reference. When a user deletes data in her Google account, Google immediately starts the process of removing it from the product and our systems as described in Google's Privacy Policy, at https://policies.google.com/technologies/retention.

16. Google users may also opt into a separate service called Web & App Activity ("WAA"). If a user turns on the WAA setting in his or her Google account with the necessary app-level and device-level permissions (*e.g.*, if the device-location setting on the mobile device is active), some activities that the user engages in while logged into her account (for instance, Google searches) are saved to that account, so the user may have a more personalized experience. For example, she may experience faster searches and more helpful app and content recommendations, such as when a user sees her search automatically suggested based on past searches.[4] Some of these WAA entries can include location information, although the source of

[4] *See, e.g.*, Google, *See & control your Web & App Activity*, https://support.google.com/websearch/answer/54068?co=GENIE.Platform%3DAndroid&hl=en (visited Feb. 27, 2020); Google Privacy & Terms, *How is location saved in my Google Account?, at Web & App Activity*, https://policies.google.com/technologies/location-data#how-save (visited Feb. 27, 2020).

the location information will vary depending on the activity, the device, and the user's other settings. LH and WAA are separate services that store data in separate databases, and there are no dependencies between LH and WAA. WAA data is not used to calculate the locations that are stored in LH, and completing a search across LH data does not search or draw on WAA data in any way.

17. Google Location Accuracy ("GLA") is a separate setting, which was formerly known as Google Location Services. It is available only on Android mobile devices. When the GLA setting is turned off, an Android device will use only GPS data to calculate its location. If a user has the GLA setting on, the Android's location services will use additional inputs, including Wi-Fi access points, mobile networks, and sensors, to estimate the device's location.[5] While location data may be periodically collected from devices with the GLA setting turned on and used in an anonymous way to improve location accuracy (*e.g.*, estimating the locations of WiFi access points and cell towers), that location data is not stored with user identifiers and is stored separately from the LH database and the WAA database.[6] As indicated, if a user has turned on GLA, then the device's location information that is sent to and stored in LH (if LH has been enabled) may be calculated using not only GPS-sourced data, but also WiFi- or cell-sourced data from the GLA database. In other words, GLA data might be used by the device to calculate a location data point that is then stored in LH. But there are no other dependencies between GLA and LH. Completing a search across LH data does not search or draw on GLA data in any way—the databases are separate and do not interact beyond the initial location calculation.

---

[5] *See, e.g.*, Google, *Manage your Android device's location settings*, https://support.google.com/nexus/answer/3467281?hl=en (visited Feb. 27, 2020).

[6] *See, e.g.*, Google Privacy & Terms, *How does Google know my location?*, at Google Location Services, https://policies.google.com/technologies/location-data (visited Feb. 27, 2020).

18. When GLA is turned on, the inputs used to calculate a user's estimated location can include WiFi access points. However, Google cannot reconstruct which WiFi access points were used to calculate a given LH data point. Although Google collects anonymized data in GLA that allows it to estimate the physical location of particular WiFi access points, and those WiFi access points in turn can be an input used to calculate a device's estimated location that is then stored in LH, Google does not know and cannot recreate which particular WiFi access points were used to calculate any particular LH data point. Google therefore cannot identify the physical location of the WiFi access points used to estimate a user's location coordinates stored in LH because it cannot determine which WiFi access points were used to estimate the user's location.

II. Google's Production of LH Information to Law Enforcement

19. I understand that this case concerns a so-called "geofence" request, which seeks LH information for all Google users whose LH information indicates that their device may have been present in a specified geographic area during a certain window of time.

20. In practice, LH is the only form of location data Google maintains that Google believes to be responsive to a geofence request, and LH is the only form of location data that was produced to the government in this case. This is because at all times relevant to this case, Google has not stored any other location information in association with specific Google user accounts that is sufficiently granular to be responsive to and searchable for such a request. To be relevant and responsive to a geofence warrant, location data must be stored in association with a specific user's account and must be able to pinpoint a user's estimated location with enough precision to bring it within the radius described in a geofence warrant. Even though Google devices and applications might sometimes use or transmit information about a user's location to

Google while the device or application is in use, no such information other than LH is stored and searchable in association with specific user accounts at a level of precision sufficient to be searched and produced in response to a geofence warrant.

21. At all times relevant to this case, WAA did not store a user's location at a level of detail precise enough to be responsive to a geofence warrant. Stored WAA data reflects a device's location to an approximate area of at least one square kilometer; and, if there are fewer than 1000 users in one square kilometer, the area is even larger. WAA data was therefore too coarse to be responsive to the warrant in this case and was not searched or produced.

22. Google does not store GLA data in association with any particular Google account. GLA data therefore is not responsive to a typical geofence warrant and was not responsive or relevant to the warrant in this case and was not searched or produced.

23. LH information can be searched in response to a geofence request. To conduct that search, Google must search across *all* LH data to identify users with LH data during the relevant timeframe, and run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant. Google does not know which users may have such saved LH data before conducting the search and running the computations.

24. The location data points reflected in LH are estimates based on multiple inputs, and therefore a user's actual location does not necessarily align perfectly with any one isolated LH data point. Each set of coordinates saved to a user's LH includes a value, measured in meters, that reflects Google's confidence in the saved coordinates. A value of 100 meters, for example, reflects Google's estimation that the user is likely located within a 100-meter radius of the saved coordinates based on a goal to generate a location radius that accurately captures

roughly 68% of users. In other words, if a user opens Google Maps and looks at the blue dot indicating Google's estimate of his or her location, Google's goal is that there will be an estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot.

25. Notwithstanding the confidence interval described above, if a user's estimated location (*i.e.*, the stored coordinates in LH) falls within the radius of the geofence request, then Google treats that user as falling within the scope of the request, even if the shaded circle defined by the 68% confidence interval falls partly outside the radius of the geofence request. As a result, it is possible that when Google is compelled to return data in response to a geofence request, some of the users whose locations are estimated to be within the radius described in the warrant (and whose data is therefore included in a data production) were in fact located outside the radius. To provide information about that, Google includes in the production to the government a radius (expressed as a value in meters) around a user's estimated location that shows the range of location points around the stored LH coordinates that are believed to contain, with 68% probability, the user's actual location.

26. In contrast, the purposes for which Google designed LH do not depend on any individual stored LH data points. For instance, the Timeline feature combines and contextualizes numerous individual stored LH data points over periods of time into inferred semantic location information (*e.g.*, place visits) so that users may store and visualize their location and movements in a journal (*e.g.*, visiting a hotel, visiting a ski resort, and driving between that hotel and ski resort). Similarly, Google may use such inferred semantic place visits (not individual stored LH data points) for ads. LH is sufficiently precise and reliable for these purposes for which Google designed LH.

I declare under penalty of perjury that the foregoing is true and correct to the best of my

knowledge and belief.

Executed this 11th day of MAR 2020, in San Francisco.

Marlo McGriff

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA v. OKELLO T. CHATRIE, *Defendant*.	Case No. 3:19-cr-00130-MHL

THIRD DECLARATION OF MARLO MCGRIFF

I, Marlo McGriff, respectfully submit this declaration in regard to the above-captioned matter. I make this declaration based on my knowledge of the facts stated herein.

1. Appended as Exhibit A and Exhibit B are documents in Google's possession responsive to the subpoena issued by the Court pursuant to Federal Rule of Criminal Procedure 17(c) on July 20, 2020 (ECF Nos. 133, 133-1) ("the Subpoena"). These documents consist of Google's subscriber registration record (the "Registration Record") and an audit record (the "Audit Record") associated with the Google Account [redacted], which I understand to be the account that is the subject of the Subpoena (the "Subject Account"). The Registration Record documents certain subscriber registration information associated with the Subject Account. The Audit Record documents user consent to Location History on the Subject Account. The information provided below is intended to translate the technical information in the Audit Record for the Court and to provide other information responsive to the Subpoena.

I. Account Creation

2. The Registration Record reflects that the Subject Account was created on August 20, 2017 (UTC) from the IP Address [redacted].

3. The Registration Record reflects that the Google Account [redacted] is associated with the numerical Google Account ID [redacted].

II. "Location History" ("LH") Setting and Location Reporting Setting

4. As I testified in my first declaration, *see* ECF No. 96-1 at 2, and as Google stated in its amicus brief, *see* ECF No. 73 at 7, a user must opt in to LH before location data can be stored in the LH service. As I also testified in my first declaration, *see* ECF No. 96-1 at 3, for LH to collect location data from a particular device, the "Location Reporting" subsetting within LH must be on for that device.

5. The Audit Record reflects that the user of the Subject Account opted in to the LH service and enabled Location Reporting for a Samsung device on July 9, 2018 at approximately 04:09 (UTC)[1] as follows:

a. The Sensorvault server recorded LH as being successfully enabled for Google Account ID [redacted].

b. Location Reporting was enabled for a device with device tag [redacted], which was a Samsung Galaxy S9 Plus (SM-G965U).

c. The user opted in to LH either through device settings or through a Google application on the Samsung device. This is indicated by the fact that Location Reporting was enabled for the Samsung device at the same time that the user opted in to LH, which can only happen when the opt-in occurs through a device-based consent flow versus a browser-based consent flow.

[1] All timestamps in the Audit Record are in standard millisecond format.

6. The Audit Record did not record the specific interface (i.e., the particular application or settings opt-in screen) through which the user enabled LH. But as of July 9, 2018 (UTC) and at all times since then, the steps and consent text necessary to opt in to LH—what Google refers to as the "supported consent flow"—have been consistent across all applications and services and across all Android devices and operating systems. Moreover, as of July 9, 2018 (UTC) and at all times since then, the Sensorvault server rejects any attempted opt-in to LH from an unsupported consent flow or device—i.e., any attempt to enable LH that does not follow the steps described here will be unsuccessful. *See* ECF No. 110-1 at 2. Because the Audit Record shows Google's Sensorvault server recording that LH was successfully enabled on the Subject Account, the user necessarily opted in through a supported on-device consent flow. If the user had encountered an unsupported on-device consent flow, the Audit Record would not show a successful enablement of LH.

7. Under the supported consent flow as of July 9, 2018 (UTC), across all applications and services, and across all Android devices and operating systems, a user who opted in to LH either directly from within device settings or when attempting to use a feature powered by LH (such as features within the Google Maps application) would be presented with an opt-in screen containing the following text:

> **Location History**
>
> Saves where you go with your devices
>
> This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON. [2]

[2] This text is the same text that would appear on the second screen I described in my

8. Across applications and services, and across Android devices and operating systems, tapping on an expansion arrow next to the text "Location History: Saves where you go with your devices" would present users with additional information about LH, which reads:

> **Location History**
>
> Saves where you go with your devices
>
> Location History saves where you go with your devices. To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, like Google Maps or Search.
>
> If you use your device without an internet connection, your data may be saved to your account once you return online.
>
> Not all Google services save this data to your account.
>
> This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google.
>
> This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

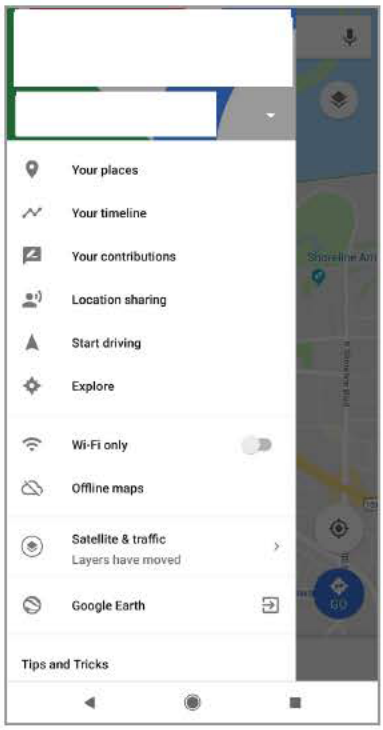
9. Tapping "TURN ON" will enable LH on the user's Google Account.

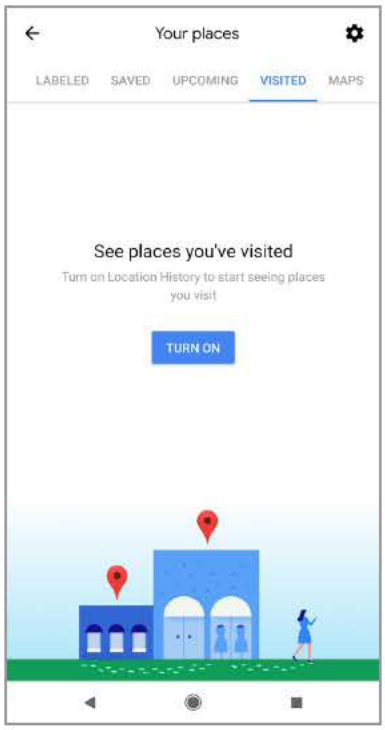
Supplemental Declaration. *See* ECF No. 110-1 at ¶ 7 ("By 2017 at the latest, it was not possible for a user to successfully enable LH solely by tapping on "YES, I'M IN" as depicted on the final screen in the McInvaille Video. Instead, a user who tapped on "YES, I'M IN" when prompted would be presented with a second opt-in screen. Only by opting in via that second screen could the user successfully enable LH for her account.").

10. The text quoted in ¶¶ 7-8 is the same text that the user of the Subject Account would have seen on July 9, 2018 (UTC), and the user would have had to tap "TURN ON" to successfully opt in to LH as reflected in the Audit Record.

11. The user of the Subject Account would have encountered this consent text and had to tap "TURN ON" to enable LH no matter what application or service the user was using when the user opted in to LH. The specific layout and appearance of that text varies depending on what application or service the user is using when the user enables LH, but the consent text and steps are the same for all apps and services. Below are examples of how that consent text could have appeared to the user.

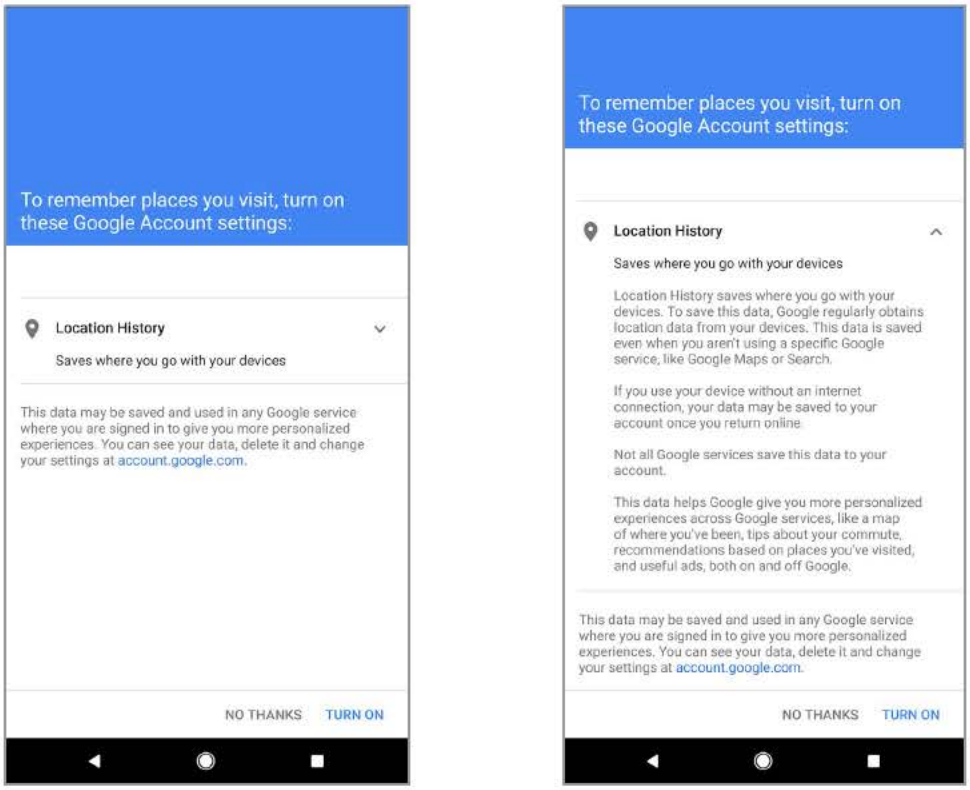
12. For example, if the user of the Subject Account navigated through the Google Maps application and selected "Your places" on the left-hand screen below, the user would have been presented with the right-hand screen below when selecting "Visited" at the top:[3]





[3] Personal identifying information has been redacted from these screenshots.

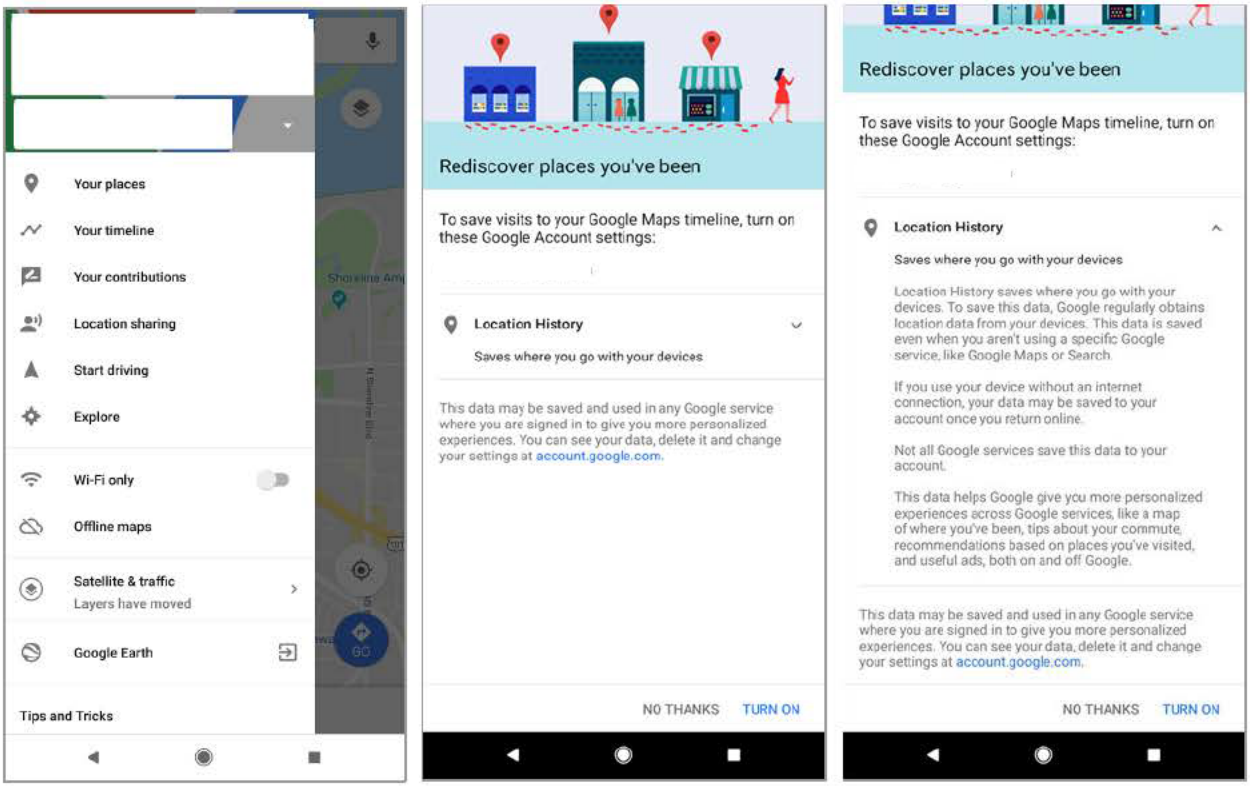
13. If the user then tapped on "Turn On" on the right-hand screen above, the user would have been presented with the left-hand screen below. And if the user then tapped on the gray expansion arrow next to "Location History: Saves where you go with your devices" on the left-hand screen below, the user would next have been presented with the additional information depicted on the right below:



14. If the user tapped "TURN ON" as shown in ¶ 13, regardless of whether the additional information was expanded, LH would have been enabled on the Subject Account.

15. Likewise, if the user of the Subject Account navigated through the Google Maps application and selected "Your timeline" on the left-hand screen below, the user would have been presented with the screen in the middle below. And if the user then tapped the gray

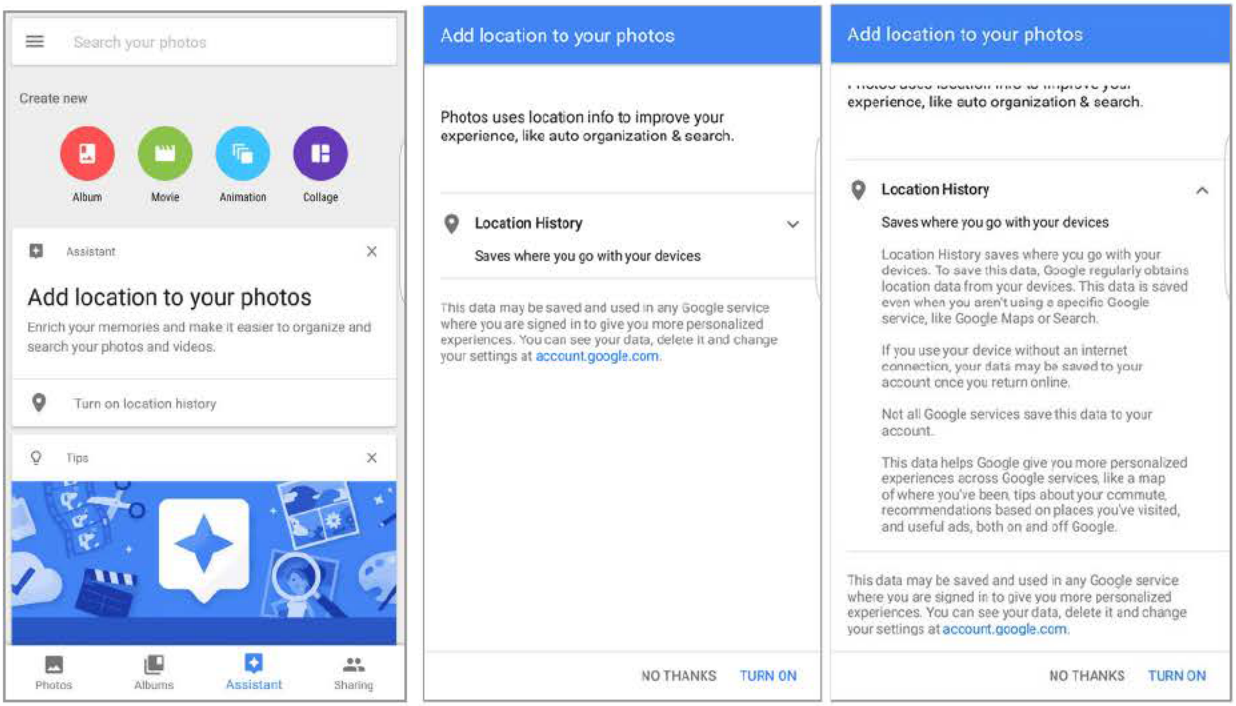
expansion arrow next to "Location History: Saves where you go with your devices" on the middle screen below, the user would next have been presented with the additional information depicted on the right below:



16. If the user tapped "TURN ON" on the middle screen (or with the additional information expanded as depicted on the right) as shown in ¶ 15, LH would have been enabled on the Subject Account.

17. As another example, the user of the Subject Account could have opted in to the LH service through the Google Photos application, as depicted by the following screens. If the user tapped on "Turn on location history" on the left-hand screen below, the user would have been presented with the screen in the middle below. If the user tapped the gray expansion arrow next to "Location History: Saves where you go with your devices" on the middle screen below,

the user would next have been presented with the additional information depicted on the right below:



18. If the user tapped "TURN ON" on the middle screen (or with the additional information expanded as depicted on the right) as shown in ¶ 17, LH would have been enabled on the Subject Account.

19. Between July 9, 2018 and May 20, 2019, monthly Timeline updates summarizing the user's monthly Location History activity (and reminding the user that the user's LH setting is turned on) were sent to users who had viewed their Google Maps Timeline (e.g., available at timeline.google.com).[4] Google has no records reflecting that such emails were sent to the user of

[4] Currently, the monthly Timeline updates are sent to all users who have sufficient monthly LH for the summaries, regardless of whether the user viewed his or her Google Maps Timeline.

the Subject Account. This could be because no such emails were sent or because the records from that time period no longer exist.

III. "Device Location" Setting

20. As I testified in my first declaration, *see* ECF No. 96-1 at 2-3, in order for a particular mobile device to send location data to LH, the device-location setting must be on for that device. Enabling the device-location setting allows the device to determine its location, which can be used by applications and services with requisite permissions.

21. On Android devices, the device-location setting is found under Android "Settings," under the "Location" menu. As of July 9, 2018, and continuing to today, an Android user has the ability to turn the device-location setting on or off.

22. Toggling the device-location setting on or off does not affect whether LH is enabled for the user's Google Account or whether the Location Reporting subsetting within LH is enabled for that device. It simply affects whether there is any location information available to be shared with LH from the device. If LH and Location Reporting have been enabled and the user turns off the device-location setting, LH and Location Reporting will remain enabled, but there would not be any location information available to be shared with LH from the device. When the device-location setting is turned back on, it would become possible for location information to be shared with LH from the device (assuming LH and Location Reporting have previously been enabled).

23. Google does not store and thus has no record of when the user of the Subject Account may have toggled the device-location setting on or off.

IV. Permitting Location Sharing With Google

24. As I testified in my first declaration, *see* ECF No. 96-1 at 2-3, on iOS devices, the user must further configure the user's mobile device to grant the required device-level location permission for an application to share location data with LH. For example, a user of an iOS device can allow Google Maps to access and transmit the device's location by toggling the location permissions for Google Maps to "Always," "While Using the App," or "Never." An iOS device can share location data with LH from a particular application only if the user sets the location permission for that application to "Always."

25. On Android devices, the number of applications that have device-level location permissions enabled impacts the frequency with which location data may be shared with LH. A user may configure applications, such as Google Maps, to access and transmit the Android device's location by toggling the location permissions for the application to "Allowed All the Time," "Allowed Only While in Use," or "Denied."

26. These location permissions are specific to each application, and toggling them does not affect whether LH is enabled for the user's Google Account or whether the Location Reporting subsetting is enabled for that device. This was true as of July 9, 2018 and remains the case today.

27. Google does not retain records reflecting when these permissions are modified for various applications and so has no record of when the user of the Subject Account may have modified these permissions for any applications on the user's device.

V. Signing in to a Google Account

28. As I testified in my first declaration, *see* ECF No. 96-1 at 3, a particular device will not report location information to LH on a particular Google Account unless the user has

signed into that account on that device. On an Android device, this means that the user must associate the user's Google Account with the device through the device settings.[5] Signing into the account through any other means, such as on a web browser, is not sufficient to allow reporting of location data to LH. Moreover, if the user has enabled LH in the user's Google Account and enabled the Location Reporting subsetting in LH for a device, but subsequently removes the user's Google Account from that device through the device settings, the device will stop reporting location to LH (even though LH remains enabled on the Google Account). This was true as of July 9, 2018 and remains the case today.

29. Google has no record showing when the user of the Subject Account may have associated or disassociated the account from the Samsung S9+ SM-G965U device.

VI. Default Settings

30. The default setting for LH at the initial account creation is "off."

31. Android devices, including a Samsung S9+ SM-G965U running Android O.S. 8.0, revision number G95USQS3BRK3, have a default setting for Location Reporting as "off," with Location Reporting for the device being enabled based on user action on the device or elsewhere.

32. The default setting for the device-location setting at the initial set-up of any Android device running Android O.S. 8.0 and earlier is "on."

VII. Version History

33. The consent text and steps I described above at ¶¶ 7-18 constituted the supported consent flow that was required to successfully opt in to LH as of July 9, 2018 (UTC), when the

[5] *See* Google, *Add or remove an account on Android*, https://support.google.com/android/answer/7664951?hl=en (visited July 22, 2020).

user of the Subject Account opted in to LH, and the consent text has remained unchanged since that time.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 30th day of July 2020, in San Francisco.

Marlo McGriff

EXHIBIT A

############## * Google Confidential and Proprietary * ###############

GOOGLE SUBSCRIBER INFORMATION

Google Account ID: [redacted]
Name: [redacted]
e-Mail: [redacted]
Alternate e-Mails:

Created on: 2017-08-20 18:04:11 UTC
Terms of Service IP: [redacted]

Deletion Date:

Last Logins: 2019-08-17 13:40:16 UTC, 2019-07-14 10:17:04 UTC, 2019-05-20 13:49:12 UTC

ACCOUNT RECOVERY

Recovery e-Mail: [redacted]
Recovery SMS: [redacted]

IP ACTIVITY

No User IP Logs

############## * Google Confidential and Proprietary * ###############

EXHIBIT B

Product: LOCATION_HISTORY
Event: LOCATION_HISTORY_SETTING_CHANGE
Component: SENSORVAULT_SERVER
UI Context: CONTEXT_ID_UNSPECIFIED
Session: (8425538384137439217, 9762534688325573142)

▾ View the complete audit record

```
event {
  name: LOCATION_HISTORY_SETTING_CHANGE
  event_details {
    sensorvault_user_preference_change {
      sensorvault_rpc_method: SET_API_SETTINGS
      location_history_setting_change {
        new_value {
          value: ENABLED
        }
      }
      sensorvault_device_preference_change {
        device_tag: [redacted]
        location_rep          ting_change {
          new_value {
            value: ENABLED
          }
        }
      }
    }
  }
}
recording_component {
  component_id: SENSORVAULT_SERVER
  server_details {
    build_label: "svfe_20180702_RC00"
    build_cl: 202963392
  }
}
timestamps {
  server_creation_time_millis: 1531189245242
}
authentication_context {
  service_loggable_security_context {
    loggable_peer {
      username: "geo-sensorvault"
      primary_role: "identity consent audit"
      unauthenticated_host: "qrpyll-v8.prod.google.com"
      jobname_chosen_by_user: "prod.identity.consent.audit.server"
      unauthenticated_borg_cell: "qr"
    }
    user {
      internal_use_only {
        scope: MDB_USER
        mdb_user {
          user_name: "geo-sensorvault"
          gaia_id: [redacted]
        }
      }
    }
    originator {
      internal_use_only {
        scope: MDB_USER
        mdb_user {
          user_name: "geo-sensorvault"
          gaia_id: [redacted]
        }
      }
    }
  }
  client_loggable_security_context {
    loggable_end_user_creds {
      loggable_credential {
        type: GAIA_MINT
        loggable_gaia_mint {
          primary_user_id: [redacted]
          loggable_credenti
            user_id: [redacted]
          }
          not_before_seconds: 1531180186
          not_after_seconds: 1531189546
        }
      }
    }
    loggable_peer {
      username: "geo-sensorvault"
      primary_role: "geo sensorvault"
      unauthenticated_host: "qlcll95 v8.prod.google.com"
      jobname_chosen_by_user: "sensorvault.stratus.prod.svfe"
      unauthenticated_borg_cell: "ql"
    }
    user {
      internal_use_only {
        scope: GAIA_USER
        gaia_user {
          user_id: [redacted]
        }
      }
    }
    originator {
      internal_use_only {
        scope: GAIA_USER
        gaia_user {
          user_id: [redacted]
        }
      }
    }
  }
}
session_id {
  uuid {
    most_significant_uuid_bits: 8425538384137439217
    least_significant_uuid_bits: 9762534688325573142
  }
}
audit_recording_server_info {
  audit_recording_component {
    component_id: IDENTITY_CONSENT_AUDIT_SERVER
    server_details {
      build_label: "borg_identityconsentauditserver_20180704.00_p0"
      build_cl: 203282562
    }
  }
}
actor_identifiers {
  gaia_user {
    gaia_id: [redacted]
  }
}
target_identifiers {
  gaia_user {
    gaia_id: [redacted]
  }
}
index_fields {
  gaia_id: [redacted]
}
```

2018-Jul-09 06:07:26 L

Product: LOCATION_HISTORY
Event: LOCATION_HISTORY_SETTING_CHANGE
Component: ANDROID_LOCATION_HISTORY_GMSCORE_MODULE
UI Context: CONTEXT_ID_UNSPECIFIED
Session: (8425538384137439217, 9762534688325573142)

1 mutation was applied.

Requested on: 2020-May-10 21:07:30 L
Mutation: One or more entity identifiers were scrubbed as part of regular Wipeout processing of ARI records. These identifiers have a special status of WIPED_OUT.

View the complete audit record.

2018-Jul-09 06:09:08 L

```
event {
  name: LOCATION_HISTORY_SETTING_CHANGE
  event_details {
    android_location_history_settings_details {
      location_history_enabled {
        value: ENABLED
      }
      location_reporting_enabled {
        value: ENABLED
      }
      source: "com.google.android.gms+opt-in"
    }
  }
}
recording_component {
  component_id: ANDROID_LOCATION_HISTORY_GMSCORE_MODULE
  device_details {
    android_device_details {
      app_package: "com.google.android.gms"
      gcore_version: "12685023"
      gcore_client_library_version: "12685000"
      device_model: "samsung SM-G965U"
      app_version_name: "12.6.85 (040400-197041431)"
      app_version_code: 12685023
      sdk_level: 26
      build_id: "R16NW"
      locales: "en-US"
      chimera_config_info {
        module_sets {
          module_set_id: "container"
          module_set_variant: 1268504
          module_targeting: 64
          module_set_version: 12685040400
          enabled_features: "brella"
          enabled_features: "brella_dynamite"
        }
      }
    }
  }
}
timestamps {
  server_creation_time_millis: 1531189348611
  client_creation_time_millis: 1531189245034
  client_upload_time_millis: 1531189347486
}
authentication_context {
  service_loggable_security_context {
    loggable_end_user_creds {
      loggable_credential {
        type: GAIA_MINT
        loggable_gaia_mint {
          primary_user_id: [redacted]
          loggable_credential {
            user_id: [redacted]
          }
          not_before_seconds: 1531189288
          not_after_seconds: 1531199648
        }
      }
    }
    loggable_peer {
      username: "identity-consent-audit"
      primary_role: "identity-consent-audit"
      unauthenticated_host: "qrsf16-v6.prod.google.com"
      jobname_chosen_by_user: "prod.identity-consent-audit-server"
      unauthenticated_borg_cell: "qr"
    }
    user {
      internal_use_only {
        scope: GAIA_USER
        gaia_user {
          user_id: [redacted]
        }
      }
    }
    originator {
      internal_use_only {
        scope: GAIA_USER
        gaia_user {
          user_id: [redacted]
        }
      }
    }
  }
  device_user_session_id: "INTV9ZKimM2dNA"
}
session_id {
  uuid {
    most_significant_uuid_bits: 8425538384137439217
    least_significant_uuid_bits: 9762534688325573142
  }
}
audit_recording_server_info {
  audit_recording_component {
    component_id: IDENTITY_CONSENT_AUDIT_SERVER
    server_details {
      build_label: "boq_identityconsentauditserver_20180704.00_p0"
      build_cl: 203282502
    }
  }
}
applied_mutations {
  timestamp: 1589137650340
  mutation_type: SOME_ENTITY_IDENTIFIERS_SCRUBBED_DURING_WIPEOUT
}
actor_identifiers {
  gaia_user {
    gaia_id: [redacted]
  }
  android_device {
    special_status: WIPED_OUT
  }
}
target_identifiers {
  gaia_user {
    gaia_id: [redacted]
  }
  android_device {
    special_status: WIPED_OUT
  }
}
index_fields {
  gaia_id: [redacted]
}
```

ATTACHMENT B

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA v. OKELLO T. CHATRIE, *Defendant*.	Case No. 3:19-cr-00130-MHL

DECLARATION OF SARAH RODRIGUEZ

I, Sarah Rodriguez, respectfully submit this declaration in regard to the above-captioned matter. I make this declaration based on my knowledge of the facts stated herein.

1. I am a Team Lead for Legal Investigations Support (LIS) at Google, where my responsibilities include processing law enforcement legal process requests directed at Google, including requests for Location History (LH) information. I joined Google in 2011 and have been in my current role since March 2018.

2. In my position, I am responsible for managing a team of LIS specialists who process and respond to certain law enforcement requests for data, including the LIS specialists involved in processing the search warrant in this case. I also process and respond to these requests.

I. Google's Production of LH Information to Law Enforcement In Response To Geofence Warrants

3. Google often receives search warrants from law enforcement authorities in the United States for a specifically identified Google user's Location History ("LH") information from a specifically identified time range. When producing data in response to such a demand,

Google searches for and retrieves only the responsive data that is associated with the particular users or accounts identified in the warrant.

4. Google also often receives search warrants from law enforcement in the United States for so-called "geofence" requests. Typically, such requests do not specify any known person, user, or account. Instead, geofence requests seek LH information for all Google users whose LH information indicates that their devices may have been present in a specified geographic area surrounding a point of interest, which law enforcement often indicates is a suspected crime scene, and a certain window of time, which might span a few minutes or a few hours.

5. Early "geofence" legal requests sought LH data that would identify all Google users who were in a geographical area in a given time frame. To ensure privacy protections for Google users and to protect against overbroad disclosures based on non-contextualized LH information, Google instituted a policy of objecting to any warrant that failed to include deidentification and narrowing measures. That protocol typically, as included in the search warrants, entails a three-step process.

6. First, law enforcement generally obtains a search warrant compelling Google to disclose a deidentified list of all Google user accounts for which there is saved LH information in a defined geographic area during a defined timeframe.

7. To comply with this first step of the process, Google must conduct the search across *all* LH data to identify users with LH data during the relevant timeframe, and run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant. Google does not know which users may have such saved LH data before conducting the search and running the computations.

8. After that search is completed, LIS assembles the stored LH records responsive to the request without any account-identifying information. This deidentified "production version" of the data includes a device number, the latitude/longitude coordinates and timestamp of the stored LH information, the map's display radius, and the source of the stored LH information (that is, whether the location was generated via Wi-Fi, GPS, or a cell tower). The volume of data produced at this stage depends on the size and nature of the geographic area and length of time covered by the geofence request, which vary considerably from one request to another. LH records are deemed responsive to a geofence warrant (*i.e.*, a user's estimated location is treated as falling within the scope of the warrant) if the stored latitude/longitude coordinates fall within the radius described in the warrant. That is true even if the shaded blue radius around those coordinates, which I understand reflects a 68% confidence interval around the location estimate, falls in part outside of the radius described in the warrant.

9. LIS deidentifies the data produced to the government at this step by removing the Google Account ID (an internal identification number assigned to the Google account that is associated to the device that is specific to each Google account) associated with the data, leaving only a device number that is used only in the Location History database. This device number is only used for distinguishing devices reporting LH to a user's account, is not a valid account identifier (as it is not unique across accounts), and cannot be mapped to an Android ID, mobile equipment identifier (MEID), or international mobile station equipment identity (IMEI) number (as it is not unique across devices).[1]

[1] An Android ID is an internal identification number assigned to each Android device connected to the Google Services Framework. *See* Google Pixel Phone Help, *Learn about the Android Device Configuration Service*, https://support.google.com/pixelphone/answer/9021432?hl=en (visited Feb. 28, 2020).

10. Second, the government reviews the deidentified production version to determine the device numbers of interest. If additional deidentified location information for a device in the production is necessary to eliminate false positives or otherwise determine whether that device is actually relevant to the investigation, law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request (if authorized in that request).

11. This additional contextual LH information can assist law enforcement in eliminating devices in the production that were not in the target location for enough time to be of interest, were moving through the target location in a manner inconsistent with other evidence, or otherwise are not relevant to the investigation.

12. Finally, based on the deidentified data produced, the government can compel Google (if authorized in the request) to provide account-identifying information for the device numbers in the production that the government determines are relevant to the investigation. In response, Google provides account subscriber information such as the email address associated with the account and the name entered by the user on the account.

II. This Geofence Warrant

13. In this case, Google received a geofence warrant (Google Reference No. 2590472) dated June 14, 2019, that was submitted to Google's online system through Detective Joshua Hylton's verified account on June 20, 2019. The geofence warrant requested information about Google accounts associated with devices that reported a location located within a 150-meter radius around a specified latitude and longitude coordinate (described as an area surrounding a Federal Credit Union and located in Richmond, Virginia) between 4:20 P.M. and

5:20 P.M. on Monday, March 20, 2019. The warrant set forth the three-step process (described above), which Google followed.

14. A LIS specialist executed the query for searching across all LH data to identify users with LH data during the specified timeframe and to run the computations against every set of coordinates in order to determine which LH records matched the geographic parameters in the warrant. The LIS specialist then produced the deidentified "production version" of the LH records responsive to the request (*i.e.*, no account-identifying information) through Google's online system to Detective Hylton's online account on or about June 28, 2019. As described above, this production included the latitude/longitude coordinates and timestamp of the responsive stored LH information, along with a display radius around those coordinates (expressed as a distance in meters) that reflects Google's confidence in the LH coordinates. A value of 100 meters, for example, I understand reflects Google's estimation that the user was likely located within a 100-meter radius of the saved coordinates based on a goal to generate a location radius that accurately captures roughly 68% of users. I understand that the same calculation would apply to any other display radius given in the production.

15. On or about July 2, 2019, Google received an email from Detective Hylton requesting additional location data (*i.e.*, step 2) and subscriber information (*i.e.*, step 3) for all 19 device numbers produced in step 1.

16. On or about July 8, 2019, Google received two voicemails from Detective Hylton. A LIS specialist called Detective Hylton that day and explained the issues in the Detective's email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant. Detective Hylton asked, and the LIS specialist explained, what information would be produced in step 2 and after in step 3. The LIS specialist also explained the importance of step 2 in narrowing. Detective Hylton stated that Google could run step 2 on

the first 9 device numbers in his email, dated July 2, 2019. Detective Hylton also stated that he would attempt to narrow further for step 3.

17. On or about July 9, 2019, Google received an email from Detective Hylton requesting additional location data (*i.e.*, step 2) on 9 device numbers.

18. A LIS specialist executed the query to search for the additional contextual location coordinates for the 9 device numbers beyond the time and geographic scope of the original request (as authorized in the search warrant). The LIS specialist then produced the deidentified "production version" of the LH records responsive to the request (*i.e.*, no account-identifying information) through Google's online system to Detective Hylton's online account on or about July 9, 2019.

19. On or about July 10, 2019, and July 11, 2019, Google received emails from Detective Hylton requesting subscriber information (*i.e.*, step 3) on 3 device numbers.

20. A LIS specialist produced the account subscriber information associated with the 3 device numbers on or about July 11, 2019.

21. On or about July 12, 2019, Google received an email from Detective Hylton requesting additional device or phone number information that could be associated with one of the accounts that LIS produced subscriber information on in step 3. A LIS specialist called Detective Hylton on or about July 12, 2019, and no further information was produced under this search warrant.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 11th day of March 2020, in San Francisco, CA.

Sarah Rodriguez



EVERY STEP YOU TAKE

How deceptive design lets Google track users 24/7

27.11.2018

FORBRUKERRÅDET

Table of contents

Table of contents **2**

1 Summary **4**

2 Introduction **4**

2.1 Method 5

3 Background **6**

3.1 Business model 7

3.2 Market share 8

3.3 Android and competition 8

3.4 Operating system functionality 9

3.5 Location tracking 10

3.6 Dark patterns and deception 12

4. Google and location tracking **13**

4.1 Location History 13

4.2 Web & App Activity 15

4.3 Setting up a Google Account 16

4.3.1 Enabling Google Assistant 19

4.3.2 Starting Google apps for the first time 19

4.3.3 Pausing Location History 22

4.4 Location tracking through Web & App Activity 23

4.5 Problematic practices 25

4.5.1 Hidden default settings 26

4.5.2 Misleading and unbalanced information 27

4.5.3 Deceptive click-flow 27

4.5.4 Repeated nudging 28

4.5.5 Bundling of services and lack of granular choices 29

4.5.6 Permissions and always-on settings 30

4.5.7 Summary of problematic practices 31

5 Legal analysis **33**

5.1 Consent 34

5.1.1 Freely given 35

5.1.2 Specific and informed? 36

5.1.3 Unambiguous? 37

5.2 Legitimate interests 38

5.2.1 Transparency 38

5.2.2 Balancing test 39

5.2.2.1 Reasonable expectations 40

5.3 Summary of legal analysis 42

6 Appendix..... 43

1 Summary

In this report, we look at how Google continuously tracks the location of its users through a number of different technologies. This tracking is implemented and enabled through the features "Location History" and "Web & App Activity". These settings are integrated into all Google accounts as a personalisation feature, and are also used to facilitate targeted advertising.

We argue that consumers are deceived into being tracked when they use Google services. This happens through a variety of techniques, including withholding or hiding information, deceptive design practices, and bundling of services. We argue that these practices are unethical, and that they in our opinion are in breach of European data protection legislation because they fail to fulfill the conditions for lawful data processing.

2 Introduction

As smartphones have become ubiquitous consumer devices, connectivity is increasingly at our fingertips at all times. Through their combination of transmitters and sensors, our phones are able to sense their environment, and pinpoint our location as we carry them around. Where we move can reveal a lot about each of us, including our religious beliefs, political leanings, and sexual orientation. It is vital that digital service providers – who are omnipresent in our lives through our smartphones – treat location data about us with care, and only collect it when strictly necessary, with our consent.

The Norwegian Consumer Council is funded by the Norwegian Government, and is an interest organisation for consumers. Part of our work is to promote consumer rights such as privacy, security and balanced contracts in digital products and services. We have published reports on how smartphone apps fail to respect consumer rights,[1] how connected devices such as toys lack basic security and privacy-protective measures,[2] and how leading digital services use unethical design choices to steer users away from privacy.[3]

[1] "Threats to Consumers in Mobile Apps" https://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps/

[2] "Internet of Things" https://www.forbrukerradet.no/internet-of-things/

[3] "New analysis shows how Facebook and Google push users into sharing personal data" https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/

This report is part of our work on consumer privacy and the right to make informed choices. Through demonstrating how users are deceived into making privacy-intrusive choices, we argue that agency is being taken away from the consumer for the benefit of service-providers. We therefore urge service-providers to avoid using deceptive practices that undermine consumers' rights to make free and informed choices.

In our previous report "Deceived by Design", we looked at how digital service providers use different unethical design practices – referred to as "dark patterns" – to lead users into making certain choices. As part of this work, we briefly touched upon the confusing layout of Google's Location History setting. As a continuation of this work, we now look closer at how Google tracks the location of their users.

Chapter 3 provides background on Google and the Android operating system, location tracking in general, and on the concept of dark patterns. In chapter 4, we identify some of the problematic practices that consumers are exposed to when setting up an Android device and creating a Google account. A legal analysis of Google's practices in light of the General Data Protection Regulation (GDPR) is included in chapter 5.

2.1 Method

In this report, we look at how several Google services collect location data from smartphone users, demonstrated through user testing. Most of the tests were performed using an Android device, with a few tests performed on an iPhone for reference. This was done through what we consider a regular user experience. When setting up a new Android device, users typically go through a process of registering and/or logging in to a Google account, and adjusting or accepting a number of settings related to data collection, such as voice data, location data, and diagnostic data. The testers documented every click and choice that appeared during the process of setting up the device, registering a new Google account, and launching the preinstalled Google apps for the first time.

The analysis and discussion throughout the report is based on European data protection legislation and ethical principles from literature on user interface



design.[4] These principles serve as benchmarks used to consider the legal and ethical aspects of the design and content of the process.

The tests in chapter 4 were performed in July 2018 using a Samsung Galaxy S7 Android device running Android version 8.0.0, which had been reset to factory settings. The results were reproduced in October 2018 on the same Samsung device, and on a Google Pixel device running Android version 9.[5] Although the settings and device setup process may vary somewhat between devices, we regard the Google account setup can to be representative of a typical user experience. The screenshots were taken in July and August 2018. A diagram that illustrates how users can turn off or avoid location tracking is included as an appendix.

Because this is an analysis of digital settings and content that may be subject to change, we cannot say with certainty that all users of these services have been presented with identical settings and design patterns during the setup process. However, our opinion is that the findings are and will continue to be relevant even if changes are made, because these examples illustrate the challenges consumers face in digital services at a given point in time.

This report was written with funding from the Norwegian Research Council through the ALerT research project[6] and the Norwegian ministry for Children and Equality. We are also thankful for invaluable help and input from the European consumer organization BEUC, the Dutch consumer organization Consumentenbond, None of Your Business (noyb), Jon Worth, Dr. Frederik Zuiderveen Borgesius, and Privacy International.

3 Background

The smartphone market is generally split between two operating systems (OS), Apple's iOS and Google's Android OS. Apple's iOS is used on all iPhone and iPad devices, while the majority of other smartphones and tablets run on a version

[4] See "Nudges for Privacy and Security", https://dl.acm.org/citation.cfm?id=3054926 and "Dark patterns and the ethics of design" https://medium.com/adventures-in-ux-design/dark-patterns-and-the-ethics-of-design-31853436176b

[5] Testers found minor differences between the Samsung Galaxy and the Pixel device, but not significant enough to change the conclusions in this report.

[6] "ALerT - Awareness Learning Tools for Data Sharing Everywhere" https://www.nr.no/en/projects/alert-awareness-learning-tools-data-sharing-everywhere

of Android. Although Apple's iOS is also popular among consumers, we have chosen mainly to focus on Google apps and Android for several reasons. These reasons are explained below, together with relevant background information.

3.1 Business model

Google and Apple have somewhat different business models.[7] Apple is primarily a hardware provider, with revenue coming from selling devices such as iPhones, with additional revenue coming from their App Store. Google makes a significant part of their revenue from data-driven advertising.[8] In 2017, Google was rated the most valuable brand in the world, with a brand value of $109.5bn /€95bn.[9]

Google is a subsidiary of Alphabet Inc., and deliver a vast amount of consumer- and business-facing services. These consumer-facing services include, but are not limited to, Google Search, Google Maps, Gmail, Android, YouTube, and Google Assistant. Google also runs a large number of business facing services, including analytics and advertising services.

Google provides most of its consumer-facing services at no direct financial cost to the user. Rather than having users pay an upfront fee for using these services, Google collects data about its users and their behavior, which is monetized through advertising and other business-facing services. Through its various services, Google collects a comprehensive picture of its users, including device information, browsing history, precise geolocation, and more. On Android devices, a large amount of data is collected passively in the background without any active actions from the user.[10]

Through compiling profiles about individual users, as well as user segments or categories based on preferences or behavior, Google can offer advertisers numerous ways to reach a target audience. Advertisers can use Google's ad

[7] "How Do Tech Companies Make Money? Visualizing Tech Giants Business Models" https://fourweekmba.com/tech-giants-business-models/

[8] "Once again, Alphabet made a lot of money on Google advertising and this time Wall Street is thrilled" https://qz.com/970765/alphabet-goog-q1-2017-earnings/

[9] "The world's most valuable brands revealed" https://www.independent.co.uk/news/business/news/worlds-most-valuable-brands-facebook-google-apple-amazon-a7556571.html

[10] A 2018 study showed that an idle Android device communicated with Google servers more than ten times as often as an idle iOS device communicated with Apple servers. "Google Data Collection research" https://digitalcontentnext.org/blog/2018/08/21/google-data-collection-research/

services to reach particular audiences with tailored ads, often called "programmatic advertising". Continued data collection about how users respond to ads, and tracking of individual users across different devices, enables Google to offer advertising spaces that are tailored to the individual user, and that are delivered "in the right moment with the right message".[11]

3.2 Market share

The Android OS is by far the dominant international market player, with an estimated 85 % of the global mobile OS market share.[12] Android is used by a variety of smartphone providers, including Samsung, Huawei, Sony, and more. Users of these phones may not be aware that Android is a Google product, and therefore that they are using a Google-powered device. Apple's iOS, on the other hand, has a market share between 10 % and 15 % globally. iOS is only available on Apple products such as iPhones, meaning that users who are using iOS already have a customer relationship with Apple.

3.3 Android and competition

Android-users have to create a Google Account before they can access the Google Play app store, which is required to download new apps, or to receive app updates. Additionally, when setting up an Android device for the first time, users have to agree to Google's privacy policy, and terms and conditions. This entails that users have to agree to Google processing user data collected through the Android device, such as device ID, usage data, and location data.

Google provides the Android OS through an open source license, meaning that the smartphone manufacturer does not have to pay Google for using or adapting Android (to develop so-called Android forks). However, the Android license agreement for manufacturers comes with a number of caveats.

While the Android OS is distributed under an open source license, the suite of apps called Google Play Services is proprietary software.[13] In order to use the Android OS on the phones they manufacture, phone manufacturers are required to include the Google Search and Google's Chrome browser

[11] "Organize audience insights" https://www.thinkwithgoogle.com/marketing-resources/programmatic/organize-audience-insights-programmatic-buying/

[12] "Smartphone OS market share" https://www.idc.com/promo/smartphone-market-share/os

[13] This includes services such as Google Play, Gmail, Google Maps, and more. "Google's Iron Grip On Android" https://arstechnica.com/gadgets/2013/10/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/

preinstalled on the phones, and use Google Search as a default search engine as a condition to use Google's proprietary apps.[14]

If, for example, Samsung were to choose not to include Google Chrome on their phones, they would be barred from including the Google Play app store. Without Google Play, users will be unable to receive app updates or install other apps on the phone without going to third party app stores.[15] Additionally, if for example Samsung were to release a phone with a competing OS on it, they would lose access to use Android on all their other phone models. In July 2018, Google was fined by EU antitrust authorities for abuse of market dominance because of these practices.[16]

3.4 Operating system functionality

Although many Google features and services are available also for iPhone users, the implementation is different between the two operating systems. Since iPhones do not come with any preinstalled Google apps, users have to actively download and activate any Google services they may want to use.[17] This also means that iPhone users do not need to have a Google account in order to download other apps.

Additionally, the app permission systems of Android and iOS are different. For example, both operating systems will ask users whether they want certain apps to access location data. However, on Android, allowing any particular app to access location data will allow the service to collect this information in the background, not just while the app is actively in use. On iPhones, users launching an app that requests location data are asked whether they want to give the app access to location at all times, or "only while using the app".[18] In other words, iPhone users can choose to give a map service access to location

[14] "EU says Google abuses its Android dominance" https://www.cnet.com/news/eu-hits-google-with-android-app-abuse-charges/

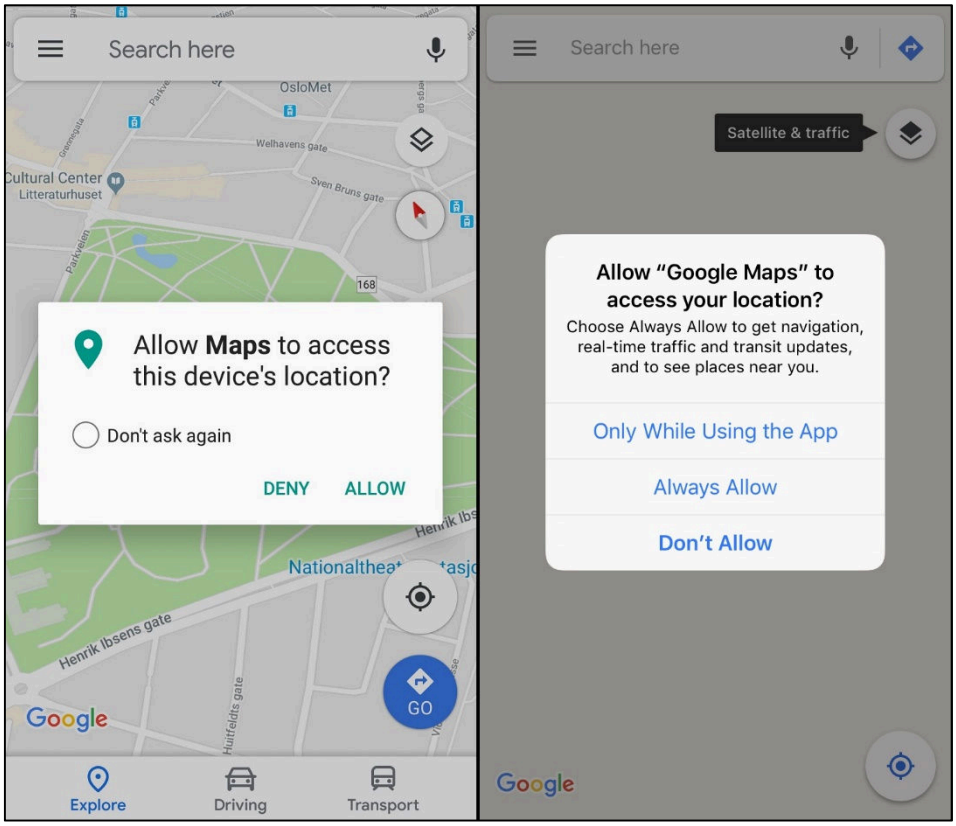
[15] "New Android OEM Licensing Terms Leak" https://arstechnica.com/gadgets/2014/02/new-android-oem-licensing-terms-leak-open-comes-with-restrictions/

[16] "Google fined £3.8bn by EU over Android antitrust violations" https://www.theguardian.com/business/2018/jul/18/google-faces-record-multibillion-fine-from-eu-over-android

[17] Except Google Search, which is set as the default search engine on iPhones. Google reportedly pays Apple between $9 and $12 billion for this. http://fortune.com/2018/09/29/google-apple-safari-search-engine/

[18] "Uber users on iPhones can now block the app from always tracking their location, thanks to Apple's new iOS update" https://nordic.businessinsider.com/thanks-to-ios-11-users-can-stop-uber-from-tracking-them-24-7-2017-9

only when they are actively using the app, while on Android users have to choose between either letting the app access location services at all times, or completely block the app from accessing location.



1 Google Maps permissions prompt. Android on the left, iPhone on the right.

3.5 Location tracking

Location data can be described as a physical position point, defined by geographical coordinates. Location tracking means that the location of a person or entity is recorded over time. When aggregated, location data can also reveal broader patterns or anomalies. As we use our smartphones for an increasing number of tasks in our everyday lives, the usefulness of location tracking is obvious. Interactive real-time maps, searches that show nearby businesses, and weather services are perhaps the most obvious examples, but location tracking can also be aggregated and used for route planning, traffic management, and so on.

It is possible to infer a lot about an individual based on their location history. Studies have demonstrated that four approximate location points is often

enough to accurately identify an individual.[19] Inferences about sensitive personal data can also be made from tracking your location. For example religious views (spends time in a mosque), political stance (attended a protest march), and health related issues (visits a cancer treatment center).

Furthermore, information about your whereabouts can reveal your habits and your personality. This can be used to target advertising, or for individualised offers and services. If you frequent a pub, indicating a drinking habit, this could be valuable information for an insurance company. Similarly, someone who regularly goes for runs could be offered lowered premiums, or be targeted by advertisements for sporting equipment. Consumers may be subjected to discriminatory practices through the individualisation of messages and offers, although these forms of discrimination can be difficult to discover.[20]

Companies such as Google are not collecting location data in a vacuum. Geolocation is part of a bigger picture, and can be combined with other data such as browsing history, preferences, social networks, shopping history, and so on. For example, information about visiting a physical store can be used to measure ad effectiveness, as long as the person who saw the ad can be identified as the same person who visited the store. This practice of combining tracking data to draw new inferences is also called "closing the loop".[21]

Consumer studies have demonstrated that consumers are particularly conscious and worried about the tracking of their location. An international 2018 study that asked more than 8000 consumers about location data and privacy, showed that 75-80 % of consumers feel vulnerable when their location data is being shared.[22] Despite this general anxiety, many consumers feel powerless to limit the amounts of data being collected through their smartphones. Consumers are also generally unlikely to adjust the privacy settings of the services they use, which makes it crucial that service-providers act responsibly when it comes to the types of data they collect, when they collect it, and how they use it.

---

[19] "Study shows how easy it is to determine someone's identity with cell phone data" https://phys.org/news/2013-03-easy-identity-cell.html

[20] In 2015, researchers at Carnegie Mellon University found that Google's advertising platform was showing higher paying jobs to more men than women. "Google's algorithms advertise higher paying jobs to more men than women" https://www.theverge.com/2015/7/7/8905037/google-ad-discrimination-adfisher

[21] "New digital innovations to close the loop for advertisers" https://adwords.googleblog.com/2016/09/New-Digital-Innovations-to-Close-the-Loop-for-Advertisers.html

[22] "Privacy and Location Data: Global Consumer Study March 2018" https://www.here.com/en/node/40306

3.6 Dark patterns and deception

As we use digital services, we are subtly being influenced in various ways, including through the user design of the service. These can be innocuous nudges, such as giving us easy access to relevant information, but some of these practices have a more insidious motive. Through so-called "dark patterns", deceptive design practices, users are nudged toward making choices that are in favor of the service-provider, and often against their own interests.[23]

Dark patterns come in many shapes, and encapsulate many different design practices. For example, the use of color, visibility and wording may serve to steer users toward choices that benefit the service provider. This can include misrepresenting the consequences of a choice, by only focusing on certain aspects that put the service provider's preferred choice in a positive light. Similarly, information that might dissuade the user from opting in to a service can be withheld or hidden from view, giving users a skewed impression.

As many mobile phone services are used on the go, users will often take the path of least resistance in order to access a service as soon as possible. Making the least privacy friendly choice part of the natural flow of a service, can be a particularly effective dark pattern when the user is in a rush, or just wants to start using the service. For example, this can be done by using a certain click-flow,[24] then subverting the design mid-flow by switching the expected function of a button. When setting up an Android device, the "Continue" button is always a blue button placed in the right corner. However, for some steps of the process, the blue button also entails enabling extra features.[25] If users are not paying full attention every step of the way, they may end up unintentionally enabling a setting without knowing that they have done so.

Furthermore, users can be deceived by being discouraged from making an active choice, paving the way for default settings that disfavor the user. When users are asked to opt out of certain settings, rather than opting in, the service-provider could be exploiting the users' disposition to leave the default settings enabled.[26] Similarly, continuous prompts that ask users to enable settings do

[23] "Dark Patterns are designed to trick you (and they're all over the Web)" https://arstechnica.com/information-technology/2016/07/dark-patterns-are-designed-to-trick-you-and-theyre-all-over-the-web/

[24] A pattern of buttons or links that have to be clicked in order to proceed through a process.

[25] See chapter 4.5.3

[26] "Do users change their settings?" https://www.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/

not respect the users' original choices, and may wear out the users and make them resign to clicking "I accept" despite originally being reluctant.

Another dark pattern entails service providers "bundling" different services that are not functionally interdependent. For example, using a map service could be made contingent on uploading your web browser history. Such bundling can make users share information that they otherwise would not, because the alternative is punishment in the form of being denied access to a service or function.

Dark patterns are often considered unethical design practices.[27] The use of deceptive design tricks to obfuscate important information, bundling, and misrepresenting what settings actually do, are also at odds with the notion of giving users agency to make informed choices. As such, dark patterns have the potential to be used in ways that circumvent laws meant to protect consumers.

4. Google and location tracking

Google mainly tracks user location through two settings, Location History and Web & App Activity, which are both integrated into the Google user account.[28] These settings can be controlled through the Google account or through Android settings, and collect and combine data from other Google Services that collect user data, such as Google Maps, YouTube, Google Chrome, and Google Photos.

In this chapter, we first give a brief overview of the Location History and Web & App Activity settings. Subsequently, we look at how these settings are presented to the user in different contexts. This is followed by a discussion of the different practices that mislead users throughout the process.

4.1 Location History

Location History is a Google account setting that continuously logs the location of the user. According to Google, the Location History feature *"helps you get better results and recommendations on Google products. For example, you can see recommendations based on places you've visited with signed-in devices, or*

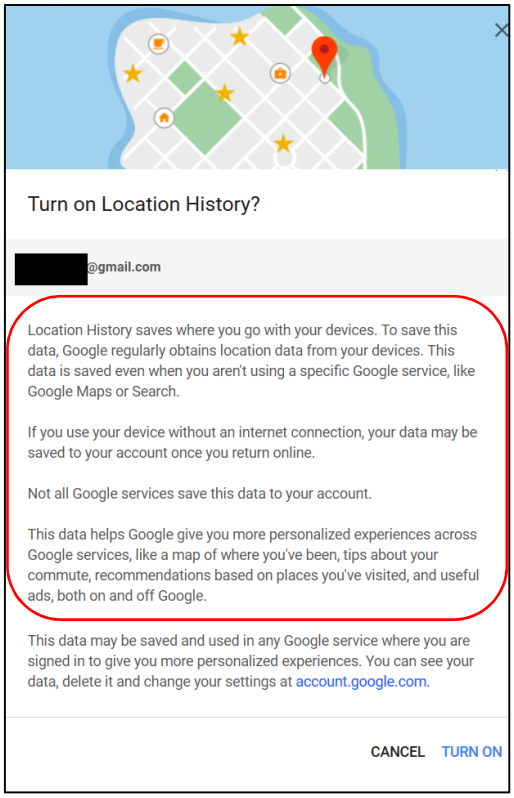
[27] "Dark patterns and the ethics of design" https://medium.com/adventures-in-ux-design/dark-patterns-and-the-ethics-of-design-31853436176b

[28] The Google user account is the main hub for most Google services, and is used to log in to Android, Gmail, Search, YouTube, and much more.

traffic predictions for your daily commute."[29] The location data collected through Location History is derived from GPS, Wi-Fi scanning, and Bluetooth scanning, which means that Google can track a user's precise location inside buildings as well as outside.

According to the description on Google's My Account website, data collected through Location History is also used to serve targeted advertising:

> *"This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google."*[30]



2 Google Location History, as seen on a Google Account.

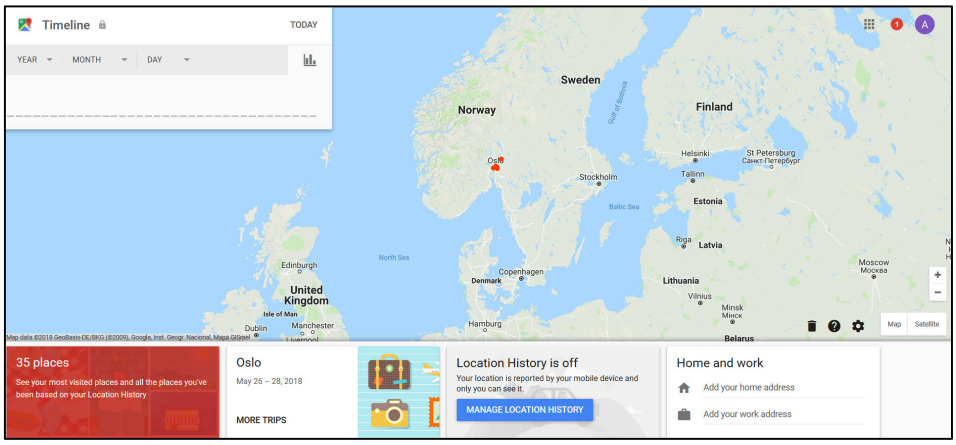
When enabled, Location History collects a variety of user data, including mode of transportation (walking, driving, on a tram, entering a vehicle, etc.), barometric pressure (altitude), Wi-Fi information, GPS coordinates, and the battery level of your device. This data is transmitted to Google, and stored as a part of the user's Google account.

---

[29] "Google Account Help - Manage or delete your Location History" https://support.google.com/accounts/answer/3118687?hl=en

[30] "Google Activity Controls" https://myaccount.google.com/activitycontrols

Some of the information inferred through this data collection (location, route, mode of transportation, which shop you visited at what time) is available on the user account ("Location History Timeline"), where users can look through their movement history for the period the feature has been enabled.[31] Other data, such as barometric pressure, nearby Wi-Fi hotspots and Bluetooth beacons, and battery level, is not visible to the user, but is collected passively in the background.



3 Google Timeline on a web browser on a PC.

According to Google, the Location History feature is voluntary, and users must opt in before the feature starts tracking user location.[32]

4.2 Web & App Activity

Web & App Activity is another Google account setting, which collects a variety of user data from an assortment of Google services. As shown in the screenshot below, Web & App Activity is described as *"Saves your searches, Chrome browsing history and activity from sites and apps that use Google services. This gives you better search results, suggestions and personalisation across Google services"*.

Google users can look at the data collected through Web & App Activity through the "My Activity" timeline on their profile, which is logged separately from the Location History Timeline.[33] This log includes timestamped records of which

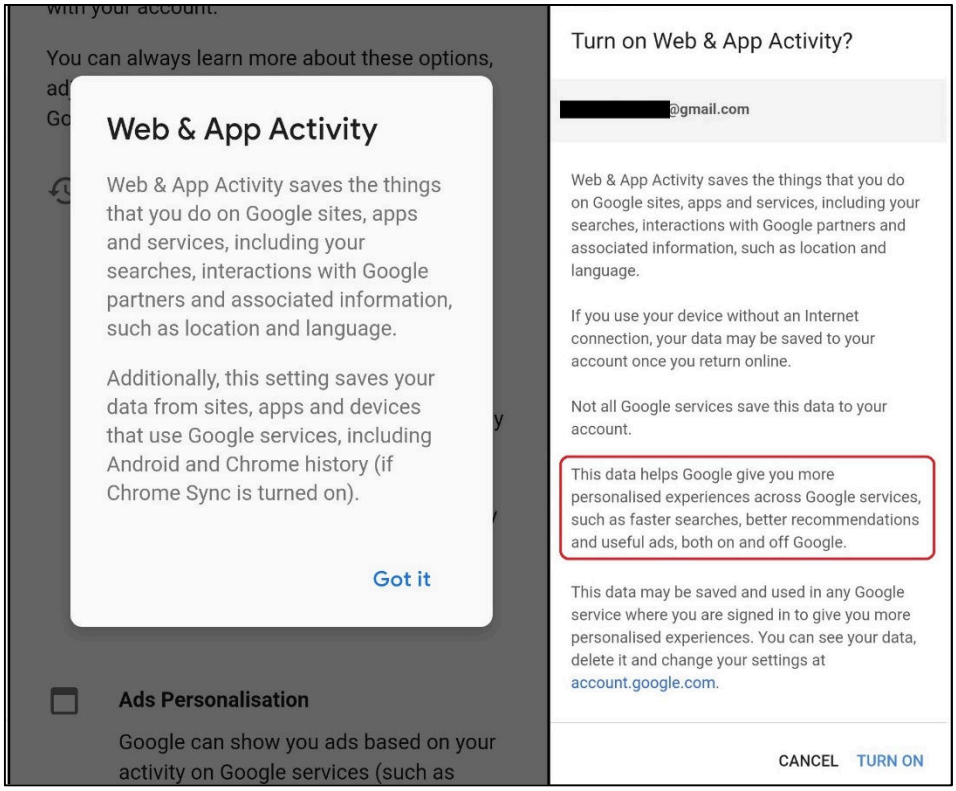
[31] "Google Timeline" https://www.google.com/maps/timeline?pb

[32] "Google privacy policy – How do I know if my Location History is on?" https://policies.google.com/technologies/location-data#is-on

[33] "Google – My Activity" https://myactivity.google.com/myactivity

apps they have used on their Android device. Web & App Activity can also track offline behavior, such as credit card purchases.[34] Web & App Activity is enabled by default when setting up a Google account.

Data from Web & App Activity is also used to personalise advertising. However, information about this data being used for advertising is only shown to the user in certain circumstances. In some contexts, such as when setting up a Google account, the use of this data for advertising is not mentioned, even after clicking "learn more". In a few limited contexts, such as when the setting has been actively turned off, and the user attempts to enable it again, Google informs the user about the advertising purposes.

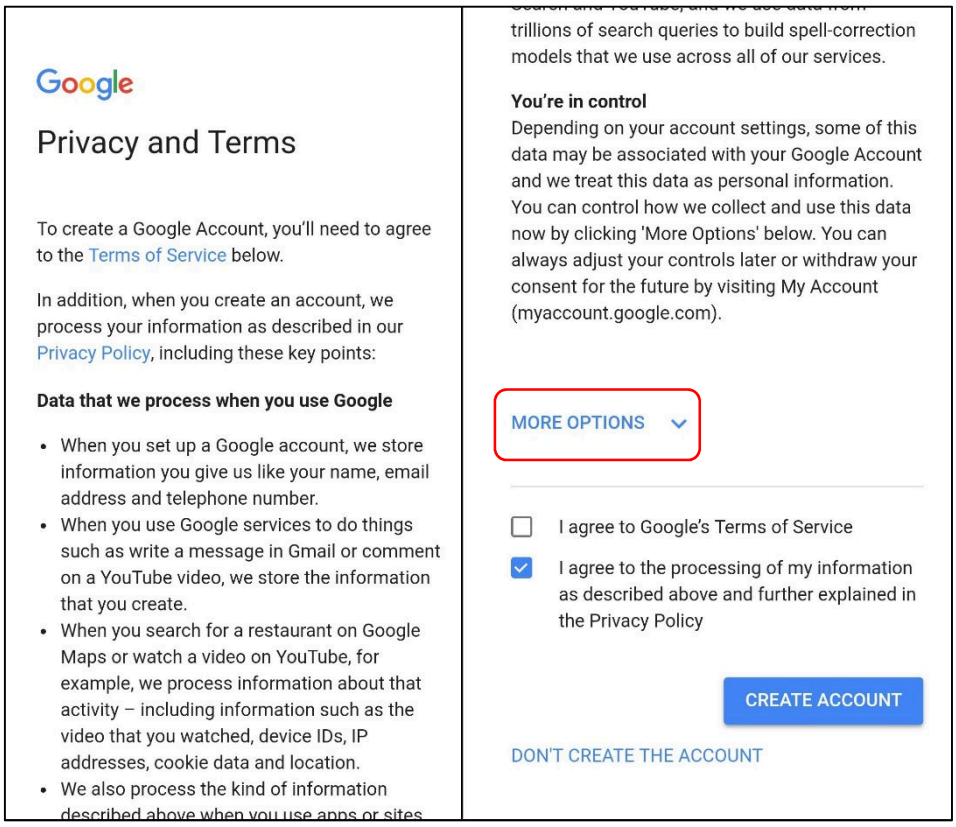


4 Information about Web & App Activity. During the Android setup process (left), and in the Google account (right).

4.3 Setting up a Google Account

When setting up a Google account, users are asked to review a truncated version of Google's privacy policy. In addition to clicking "Create Account", users can click "More options", which reveals a number of settings that can be adjusted.

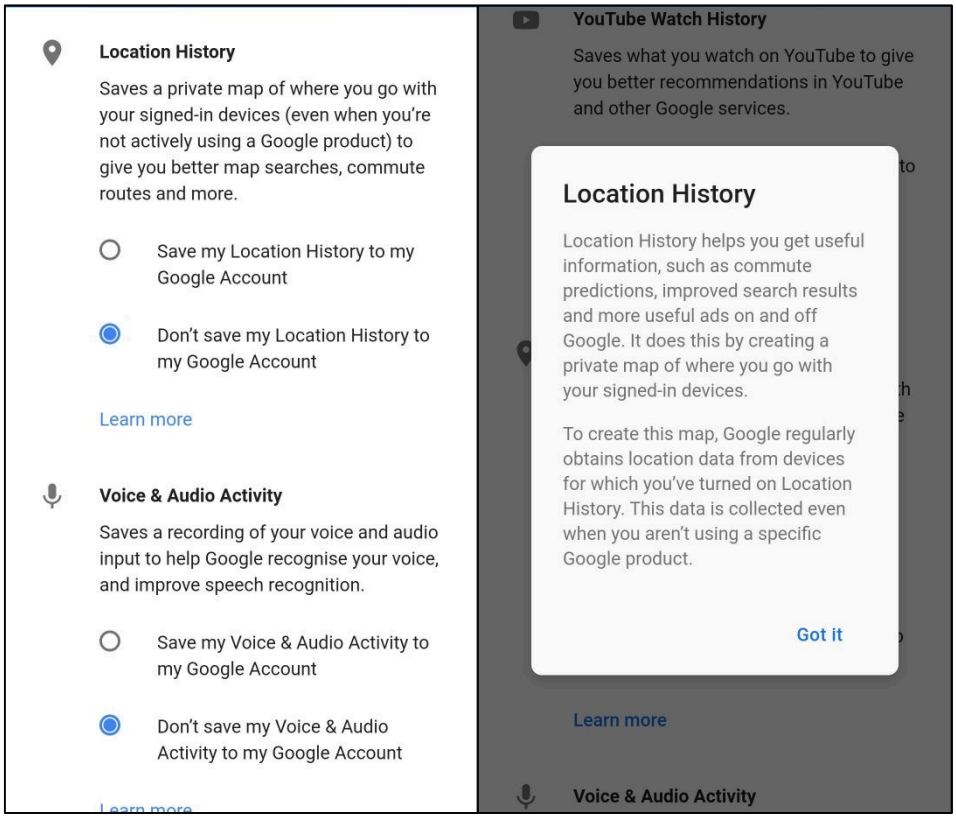
[34] "How to use Google privacy settings" https://www.consumerreports.org/privacy/how-to-use-google-privacy-settings/



5 Users have to click "More options" to adjust the Google settings.

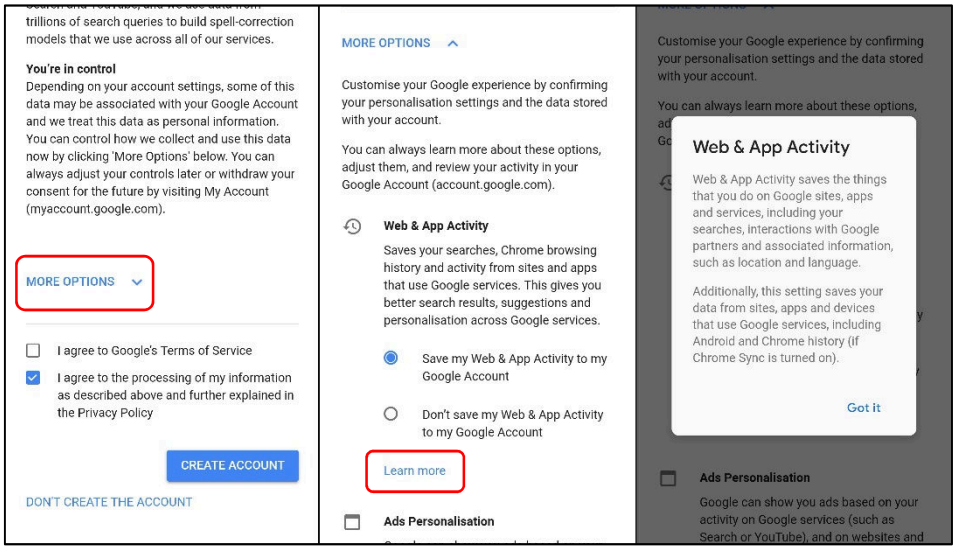
As the screenshot below illustrates, Location History is turned off by default when setting up the account. Note that there is no clear indication that this information is also used for advertising purposes, unless the user clicks “Learn more”. Clicking “Learn more” reveals that the location data collected through Location History is used to serve “more useful ads on and off Google”.[35]

[35] Screenshot of the whole screen and text is included in the appendix.



6 Location History when setting up a Google account.

After clicking "More options", it is also revealed that Web & App Activity is turned on as a default setting. The description beneath the setting says that it provides "better search results, suggestions and personalization". Note that there is no obvious indication that Web & App Activity will record location data, unless the user clicks "Learn more". Neither text mentions advertising.

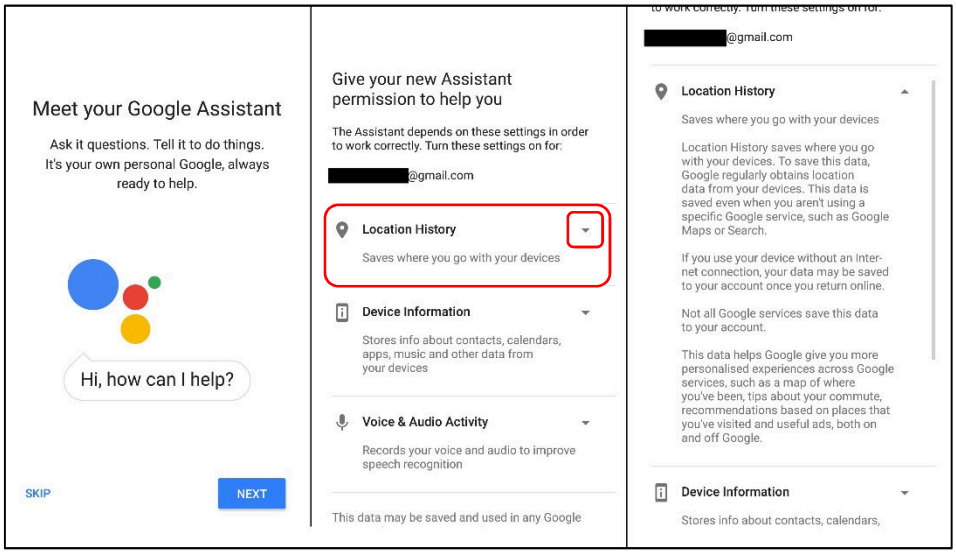


7 Web & App Activity is enabled by default.

4.3.1 Enabling Google Assistant

As part of the process of setting up an Android device, users are asked to enable a service called Google Assistant. Google Assistant is a voice-activated digital assistant, meant to help users perform everyday tasks. The assistant is also an integral part of the Google Home smart speaker system, and several other products made by both Google and third parties. This means that the Google Assistant is likely to become a fixture in the everyday life of many consumers.[36]

As the screenshots below shows, enabling the Google Assistant service in the Android setup process, also entails turning on Location History. On this screen, users are only told that Location History "saves where you go with your devices". If the user clicks the inconspicuous grey arrow to the right of Location History, a more detailed description appears, including the fact that the data is used for advertising purposes.



8 Google Assistant prompt, when setting up an Android device.

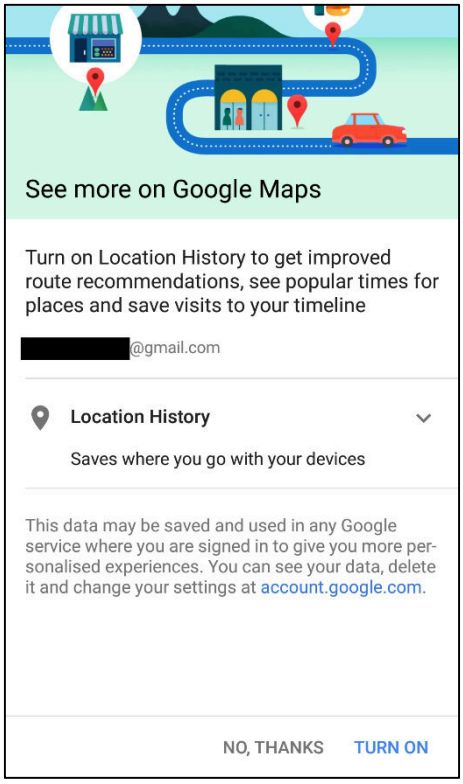
4.3.2 Starting Google apps for the first time

If the user has not enabled Location History when setting up their Android device, they will be asked to enable the setting on several other occasions.[37]

[36]"Google Assistant" https://assistant.google.com/platforms/speakers/

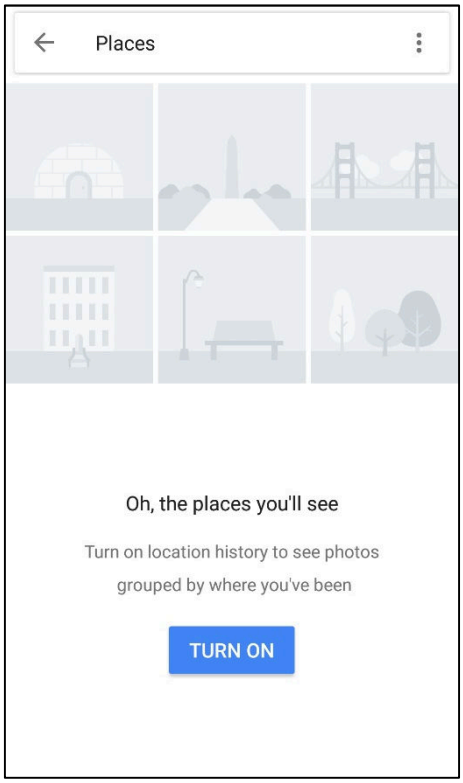
[37] For this test, we only tried starting the preinstalled Google apps after a fresh Android install. We did not observe prompts to enable Location History during the startup of the Google apps YouTube, Chrome, Hangouts, and Drive.

Upon opening the Google Maps app for the first time, users are asked again to activate Location History. The pop-up says that Location History will give users "improved route recommendations, see popular times for places and save visits to your timeline". Unless the user clicks the inconspicuous arrow on the right, they will not be informed that this information is also used for marketing purposes.



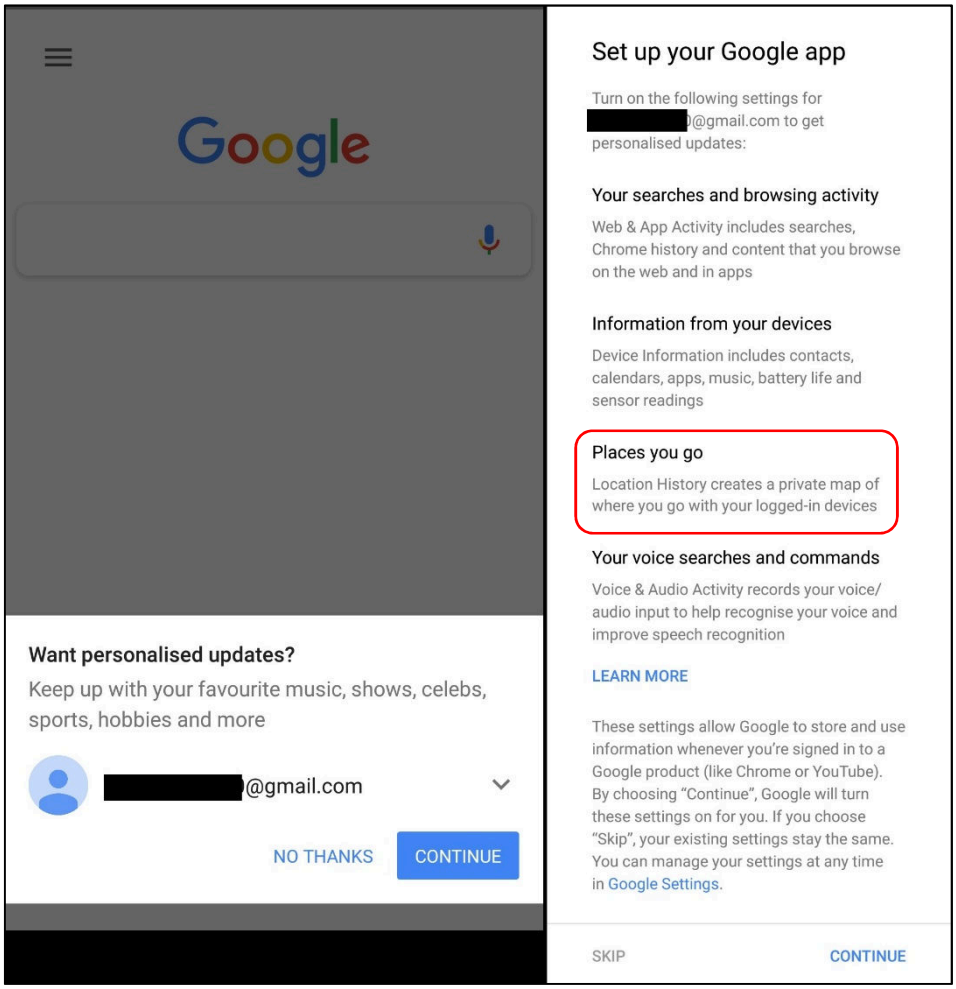
9 Location History prompt when opening Google Maps.

Upon opening the Google Photos app and clicking the "Places" gallery button, users are also asked to turn on Location History. According to Google, enabling Location History lets the user "see photos grouped by where you've been". It does not appear to be possible to enable this particular feature without enabling Location History.



10 Location History prompt when opening "Places" in Google Photos.

Upon opening the Google App for the first time, users are asked once more to enable Location History. As the screenshot below shows, there is no visible information about what enabling Location History actually entails, and there is no obvious button to display more information about Location History before activating the service as a part of “personalised updates”.

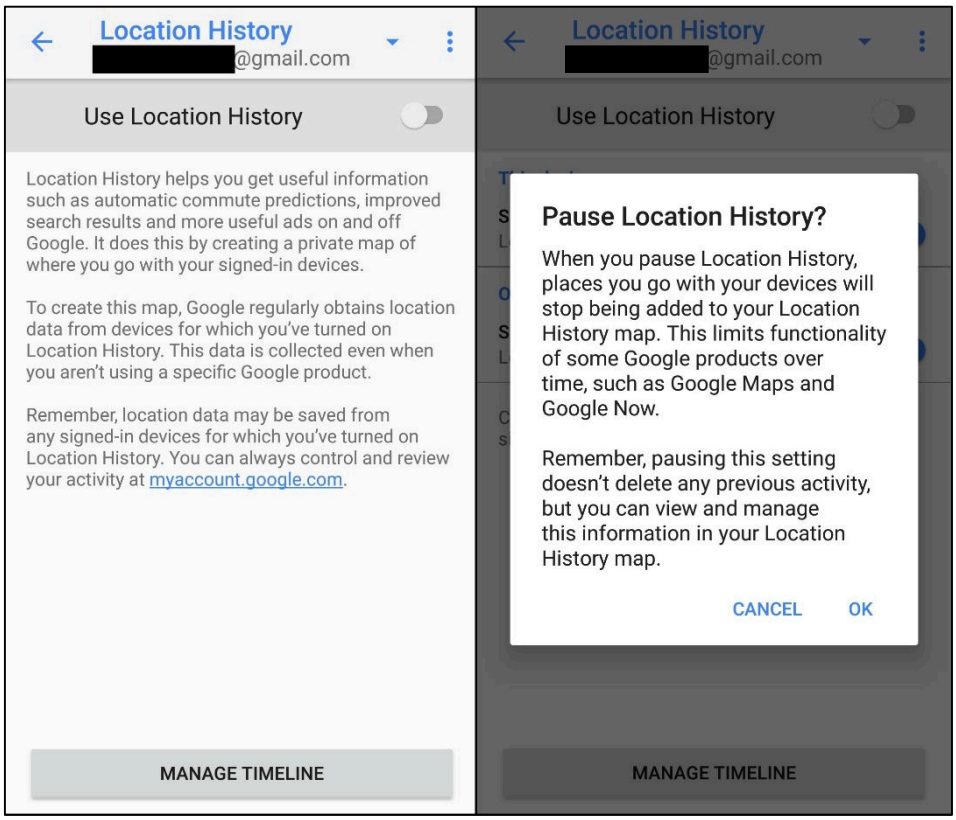


11 Popup when opening Google App for the first time.

4.3.3 Pausing Location History

It is possible to turn Location History on, or to pause it, in the Android location settings menu. As the screenshots below demonstrate, the information given here is somewhat truncated, but informs users that the data collected through Location History is used for ads.

Attempting to pause the service results in a warning that pausing it "limits functionality of some Google products over time". However, there is no comprehensive explanation of all services that are affected, or how their functionality will be limited.



12 Location History in Android settings.

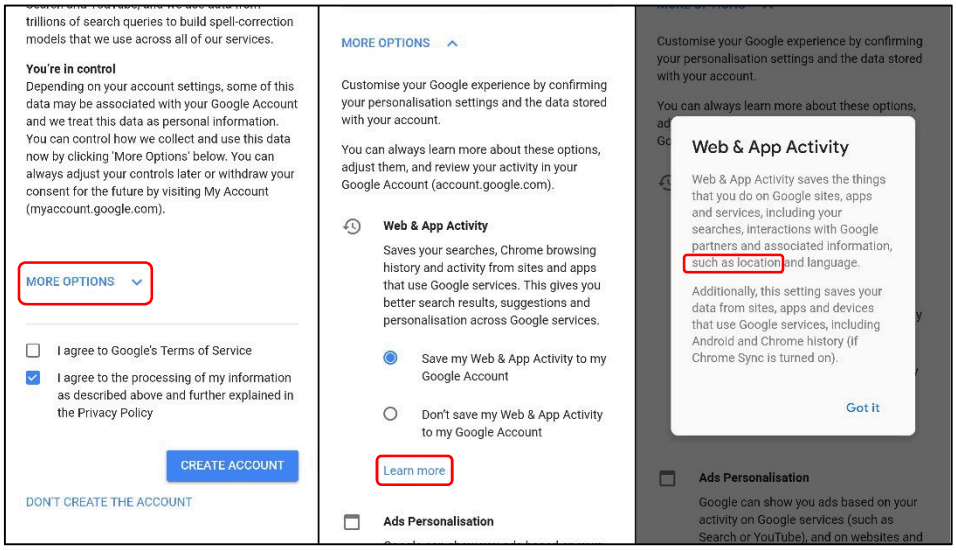
It is also worth noting that there is no real option to *turn off* Location History once it has been enabled; users can only *pause* it after the Google account has been created. This raises questions about whether the user has actually withdrawn his or her consent to the use of past location data for advertising, or if pausing Location History only halts the collection of future data. The process of deleting historical location data is separate from pausing Location History, and Location History data is seemingly retained indefinitely if the user does not actively delete it.[38]

4.4 Location tracking through Web & App Activity

If the user has purposefully avoided enabling Location History, this does not necessarily mean that Google is not collecting the user's location. A report published by the Associated Press in August 2018 showed that Web & App Activity also reports user location data to Google, which is used for

[38] In March 2017, the Danish Consumer Council filed a complaint with the Danish data protection authority against Google. This complaint alleges, amongst other things, that Google retains Location History data indefinitely without a sufficient legal reason to do so. "Forbrugerrådet Tænk anmelder Google til Datatilsynet» https://taenk.dk/om-os/presserum/forbrugerraadet-taenk-anmelder-google-til-datatilsynet

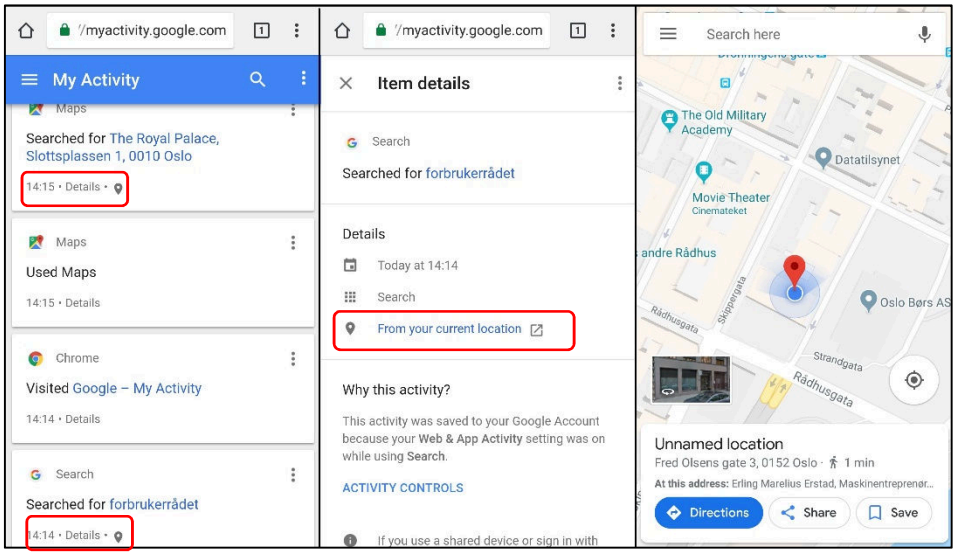
personalisation purposes such as advertising.[39] As mentioned, Web & App Activity is enabled by default when setting up a Google account. Unless the user first clicks "More options", and then "Learn more", it is not clear that this setting actually collects location data.



13 Web & App Activity when registering a Google account.

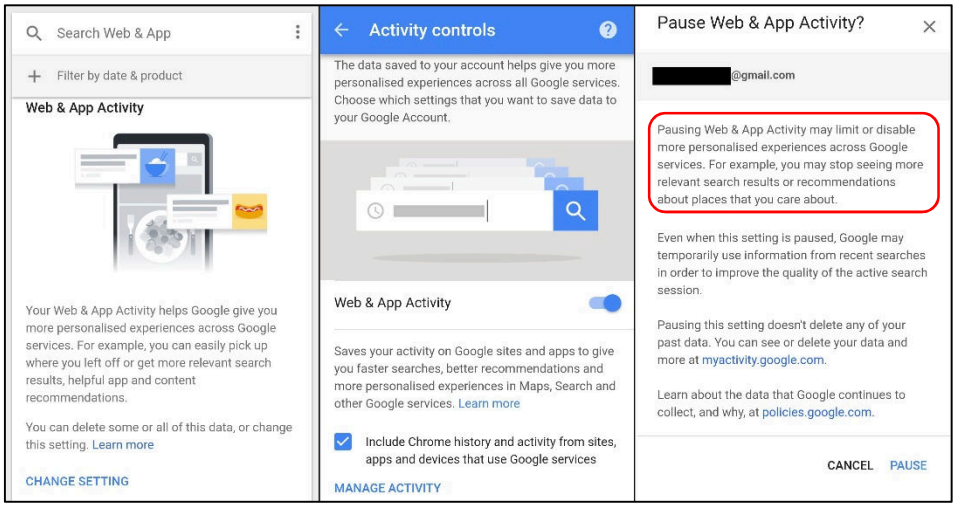
Although most apps do not record the user's location through Web & App Activity, certain apps and services, such as Google searches and searches made through Google Maps, are logged with location data of where the user was when he or she performed the search. In other words, users who turn Location History off, but leave Web & App Activity on, will still have some of their location data collected by Google. Location data logged through Web & App Activity is not visible on the timeline map that Location History provides, but shows up if the user looks at the My Activity timeline, which is wholly separate from Location History.

[39] "Google tracks your movements, like it or not" https://apnews.com/828aefab64d4411bac257a07c1af0ecb



14 Location data recorded through Web & App Activity

As with Location History, users who attempt to pause App & Web Activity receive a vague warning that this will limit or disable functionality. This non-extensive list includes “you may stop seeing more relevant search results or recommendations that you care about”.



15 Pausing Web & App Activity

4.5 Problematic practices

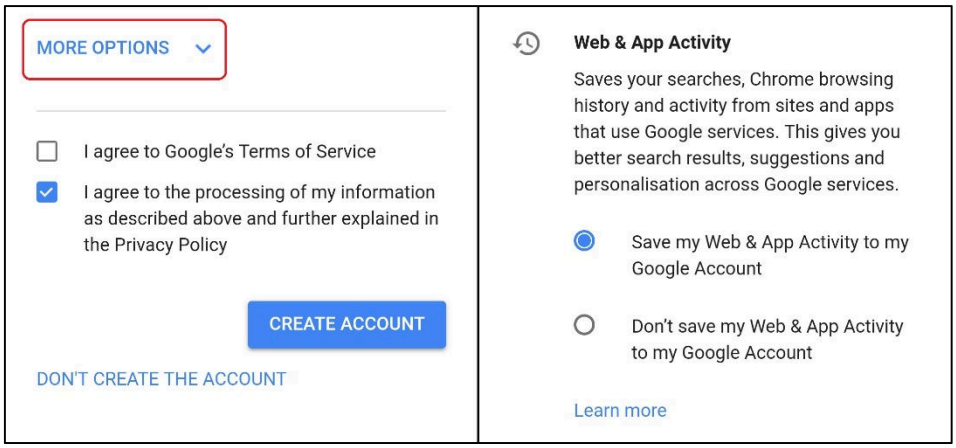
As outlined above, we see a number of problematic ethical and legal issues with the ways that Google have implemented Location History and Web & App Activity into the Google account and the Android operating system, and how they present these settings to the user. In the following, we expand upon the problematic issues, followed by a legal analysis of how the issues are, in our opinion, at odds with the GDPR.

Google give a certain degree of control to the user through its account system. For example, Location History can be deleted through the Location Timeline, and can be exported through Google's "Takeout" tool.[40] However, the data extracted through Takeout seems to be more detailed than what is shown in the Location History timeline.[41]

Users that delve into the dashboard can also get a certain degree of control over what ads they see.[42] Additionally, there is a lot of different information and settings spread throughout the Google dashboard, although some of these can be difficult to find.[43]

4.5.1 Hidden default settings

When setting up a Google account, the actual account settings are hidden behind extra clicks. Users first have to click "More options" to see what the settings are, and whether they are enabled or disabled. Web & App Activity is enabled by default, meaning that users who did not click "More options" will not be aware that this data collection is happening.



16 Default settings hidden behind "More options".

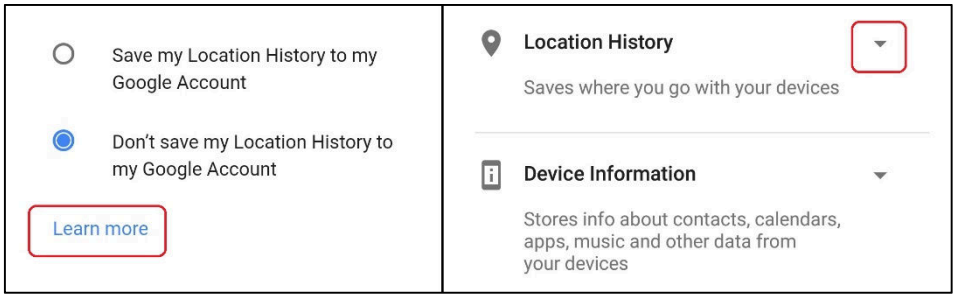
Users are unlikely to diverge from default settings, either because they are in a rush to use a service, or because they trust the service-provider. In any case,

[40] Google Takeout https://takeout.google.com/settings/takeout
[41] This can be seen by using third party tools such as Location History Visualizer https://locationhistoryvisualizer.com/
[42] Google Ads Settings https://adssettings.google.com/
[43] In "Deceived by Design", we documented some of the hurdles of navigating through the Google account dashboard. See pp. 34-39 https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

obscuring the invasive default settings is a dark pattern that dissuades users from making an active choice, and does not provide data protection by default.

4.5.2 Misleading and unbalanced information

Whenever the Location History and Web & App Activity settings are presented to the user, the clearly visible information is limited to a few positive examples of what the setting entails. The information that is visible often also trivializes the extent of tracking that is going on, and how it is used. For example, in all the instances where users are asked to enable Location History, the fact that this data is also used for advertising is hidden behind a grey arrow or a "Learn More"-link.



17 Relevant information hidden behind extra clicks.

Similarly, the fact that Web & App Activity collects location data is also always hidden behind another click, and information about this data being used for advertising is only available in some contexts. Consequently, users are not given sufficient information to make an informed choice. This appears to be cherry picking from the service-provider's side, where certain aspects that may be perceived as negative by the user are glossed over.

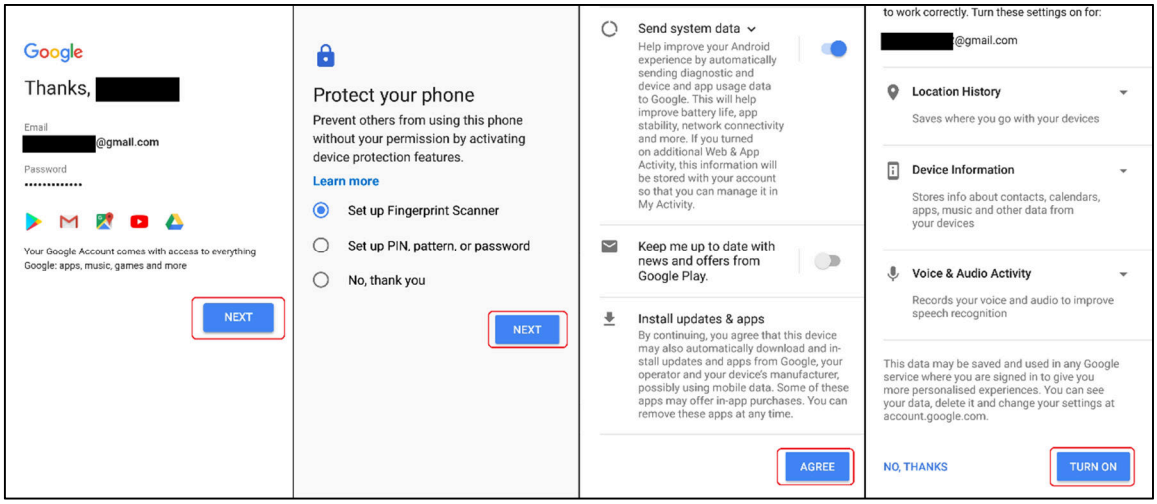
Even if the user clicks "Learn more", the description of both Location History and Web & App Activity still seems to mislead the user about what they are actually agreeing to. For example, Location History is often described as being a "private map", which may give the impression that the information is not used for other purposes such as advertising. Similarly, the name "Web & App Activity" obscures the fact that the setting also collects location data.

4.5.3 Deceptive click-flow

Although Location History technically has to be enabled before it begins collecting data, users following the click-flow when setting up an Android device are likely to unknowingly enable the setting. Google has designed the Android

setup choice-architecture in a way that facilitates enabling Location History as part of the setup process.

As shown below, throughout the setup process, the way to proceed is represented by blue buttons on the bottom right of the screen. However, if the user keeps clicking the blue buttons throughout the process, they will also enable Google Assistant, which means that Location History is also turned on. In other words, users that do not want to share their location with Google have to be very attentive in order to stop location tracking. This is a dark pattern that may end up both irritating and confusing a potentially impatient user into enabling Location History without being aware of it.

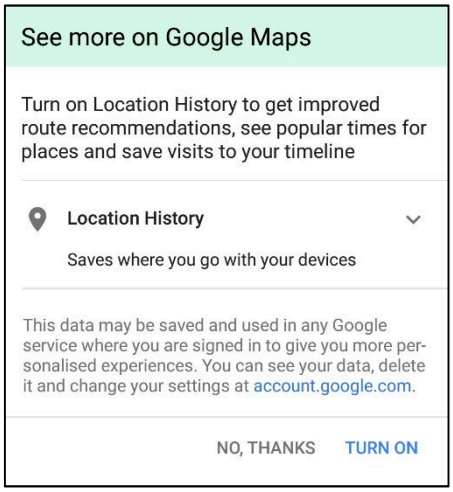


18 Some steps from the Android setup process. Google Assistant prompt on the right. Note that this is a shortened version of the actual process.

4.5.4 Repeated nudging

Users are repeatedly asked to turn on Location History, in many different contexts. On Android devices, users that do not wish to enable Location History have to decline the setting at least four times when using different services that are preinstalled on Android phones;[44] in Google Assistant, Google Maps, Google app, and Google Photos.

[44] Google Maps and Google Photos also ask users to enable Location History on iPhones, but since iOS has different preinstalled services, we regard the nudging as more pressing on Android devices.



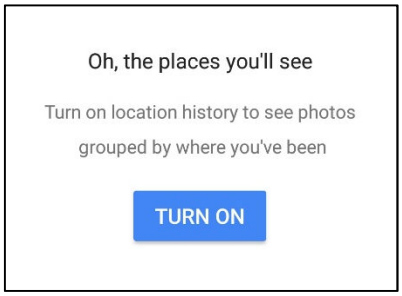
19 Prompt in Google Maps to enable Location History.

Instead of Google taking "no" for an answer, users have to keep making the same choice repeatedly. This increases the chances that users turn on the setting, either by accident, because they are tired of being asked, or because they believe that the services will not work otherwise.

4.5.5 Bundling of services and lack of granular choices

Throughout the Google ecosystem of services, separate services or functionalities are integrated and co-dependent, or simply bundled together. Enabling Location History is required in order to enable other services that users may want to use, such as Google Assistant and Google Photos Places.

Having your photos grouped by location may be a useful and desirable feature for many users. However, in order to enable this feature, users must also enable Location History. There is no granularity to this choice, meaning that users that want their photos grouped by location can only receive this feature by opting in to location tracking for advertising purposes.



20 Prompt in Google Photos to enable Location History.

Similarly, when enabling Google Assistant as part of the Android setup process, users also have to enable Location History. Despite this, the Google Assistant

service appears to function even if the user later disables Location History, although the user is never informed about this.[45]

Conversely, there is no granularity to the actual Location History setting. Either users have to allow Google to collect their location data at all times through Location History, or they must reject the feature in its entirety, blocking off other services that have Location History bundled into them.

In other words, if the user does not allow Google to collect user location data at all times through Location History, Google appears to block off potentially useful features such as Google Assistant and photos sorted by location. This all-or-nothing choice benefits Google at the cost of failing to respect users by for example providing granular choices.

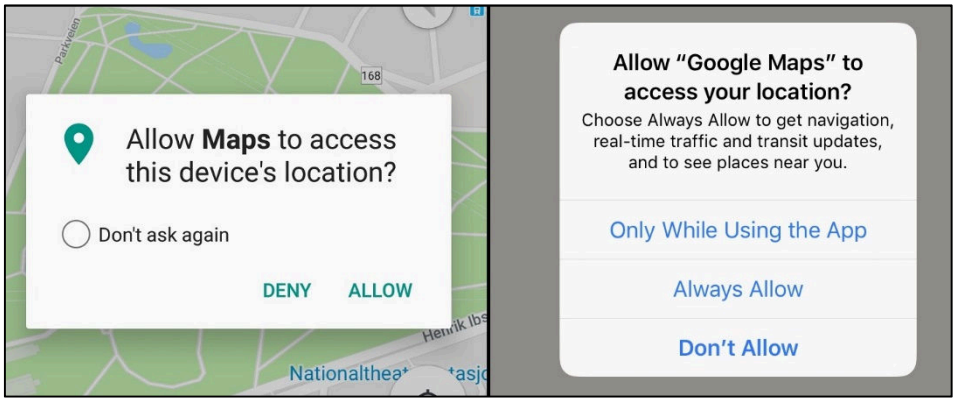
4.5.6 Permissions and always-on settings

When enabled, Location History is always on in the background on Android devices, regardless of whether the user is actively using a service that requires location services. In part, this seems to be because of how the Android operating system works.

Android users that want to use an app that requires location data, have a binary choice; Either they give the app permission to use location services, in which case the app can also record user location when the app is not in use. The alternative is to deny the app permission completely, which means that the app cannot use location services even when in active use.

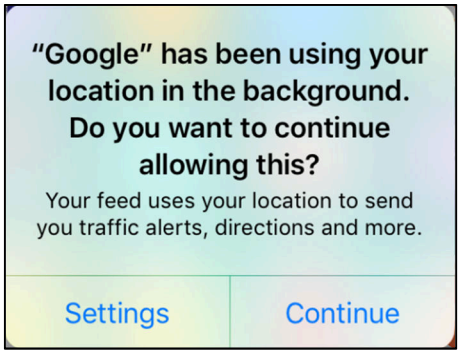
On iPhones, on the other hand, users can choose to give an app permission to use location services only when the app is in use. The latter practice is an example of privacy-preserving technology, while Google's solution is an all-or-nothing choice that limits the users' options.

[45] "If you're using an Android phone, Google may be tracking every move you make" https://qz.com/1183559/if-youre-using-an-android-phone-google-may-be-tracking-every-move-you-make/



21 Device level permissions. Android on the left, iOS on the right.

Additionally, if the user has allowed an app to access location in the background, iOS will periodically remind the user that this is happening. This prevents the user from enabling tracking in one context for a specific reason, then forgetting to turn it off.



22 iOS reminder that the user has given the Google app access to location, even when the app is not in use.

4.5.7 Summary of problematic practices

As users rarely change their settings or break the click-flow when installing software, many are likely not to realize that they turned on Location History,[46] or that Web & App Activity is enabled. Through a variety of dark patterns, Google is getting a blanket permission constantly to collect the exact location of the user, including the latitude (e.g. floor of the building) and mode of transportation, both outside and inside, to serve targeted advertising.

Users that are setting up their Android device, and are eager to get the device up and running, are particularly susceptible to inadvertently turning on Location History, while anyone who want to use Google Assistant when setting up their

[46] In July 2018, Google began sending monthly emails to users with Location History movement. These emails give some aggregated information about the user's monthly travels, but do not mention any other ways that this data is being used.

Android device will end up enabling this pervasive tracking. Furthermore, if the user has kept Location History disabled despite the continued nudging, his or her location will still be shared with Google through Web & App Activity.

In our opinion, the sum of these practices is that users are deceived into enabling privacy adverse features. This deception is unethical, and fails to respect user agency. In the following chapter, the practices will be discussed in the context of European data protection legislation.

5 Legal analysis

In this chapter, we examine whether Google has fulfilled the legal requirements under the GDPR when using location data collected through "Location History" and "Web & App activity" for advertising purposes. For the purposes of this chapter, the terms "data subject" will be used interchangeably with "user", and "data controller" will be used to mean Google.

As demonstrated in chapter 3.5, location data is personal data – information that directly or indirectly can identify a natural person.[47] This means that Google is collecting personal data when it collects and stores information about a person's location and movement through "Location history" and "Web & App activity".

The processing of personal data is only lawful if one out of six general terms is fulfilled.[48] When considering the legal grounds for Google's processing of location data for advertising purposes, we will therefore begin with establishing what legal basis Google is using. In order to establish this, we have used Google's European privacy policy as the main source.[49]

From the privacy policy, it appears that Google is relying both on user "consent" and on "legitimate interests" when processing location data for advertising purposes.[50] It is not clear from the privacy policy which legal grounds applies to what manners of processing. This is in itself problematic, as Google has an obligation to be specific about what legal grounds it is using for particular processing of personal data.[51] Relying on legitimate interest to process data while the processing could have been based on another lawful basis, also constitutes a violation of transparency requirements.[52]

---

[47] GDPR art. 4(1)

[48] GDPR art. 6. See also GDPR recital 40.

[49] "Google privacy policy" https://policies.google.com/privacy#enforcement

[50] On the basis of Google's European privacy policy, this report will not consider other legal grounds than "consent" and "legitimate interest" in art. 6 GDPR for Google's processing of personal data through Location history and Web & App activity

[51] As a result of an investigation done by the EU Data Protection Authorities, Google was already in 2012 urged to clarify which legal basis it uses for processing of personal data. See https://www.cnil.fr/sites/default/files/typo/document/20121016-letter_google-article_29-FINAL.pdf and https://www.cnil.fr/sites/default/files/typo/document/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf

[52] GDPR art. 5(1)(a) see also https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/

To be compliant with GDPR, consent has to be opt in. Because Location History is based on users opting in (off by default), we will assume that this data processing is based on consent.[53] Web & App Activity is turned on by default, and we anticipate that Google cannot rely on consent as a legal basis. The Article 29 Working party clearly state that "pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement" is invalidate consent under the GDPR.[54] Therefore, we assume that processing of location data collected through Web & App Activity is based on legitimate interests.[55]

In the following we analyze whether the way that Google collects consent for Location History is in accordance with the requirements set forth in the GDPR. This is followed by a discussion of the legal grounds for Web & App Activity.

5.1 Consent

Consent is defined in the GDPR as "any freely given, specific, informed and unambiguous indication" by a "statement" or by "clear affirmative action" from the data subject.[56] All of these conditions need to be fulfilled for consent to be considered valid. Below we will look at whether Google's use of Location History data for advertising purposes fulfills these conditions.

In Google's privacy policy, it states:

> "*We ask for your agreement to process your information for specific purposes and you have the right to withdraw your consent at any time. For example, we ask for your consent to provide you with personalized services like ads. We also ask for your consent to collect your voice and audio activity for speech recognition.*"

From this, it appears that Google is relying on consent as a legal ground for at least some of its processing of personal data, particularly for serving targeted advertising.

---

[53] GDPR art. 6 (1)(a). See also art. 5(3) of the ePrivacy Directive which requires consent to pull information from a user's device. As the ePrivacy Directive already requires consent for reading information (such as location data) from a user device, it makes most sense if the applicable legal basis under the GDPR is also consent in Location history.

[54] Working Party 29"Guidelines on Consent under Regulation 2016/679" p. 16. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

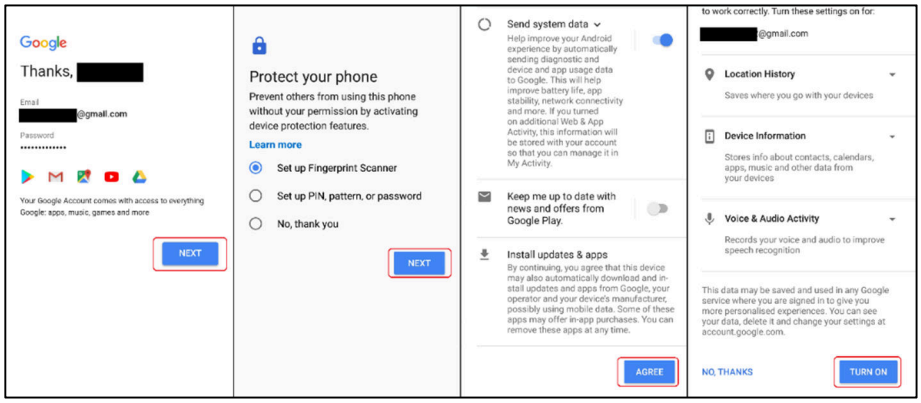
[55] GDPR art. 6(1)(f)

[56] GDPR Art.4(11)

5.1.1 Freely given

Since, as Google argues, users have to opt in to Location History,[57] the data subject should freely have given his or her consent for processing of personal data collected through Location History. This indicates that the data subject has been provided with a real choice about whether he or she accepts Google processing such data, and that this data may be used for advertising purposes.

However, as demonstrated in chapter 4, there are significant differences in how Google collects consent for Location History between iOS-users and Android users. During the Android setup process, users are guided through a process that seems designed to make users consent to Google processing their location data, simply by following the click-flow.



This click-flow makes the user likely to enable Location History as a part of the process, without being made fully aware of what this entails. If the user was not aware what he or she consented to, it will be contestable whether consent has been freely given. Furthermore, if the user has not given consent to Location History during the setup process, Android users are nudged toward enabling the setting at several other occasions. The user may feel pressured into giving his or her consent because of this recurrent nudging.

This is problematic, considering consent should be freely given in order to be valid. "The Article 29 Working Party" have stated that consent is not freely given if there is "any element of compulsion, pressure or inability".[58] Additionally,

[57] "Google privacy policy" https://policies.google.com/technologies/location-data#is-on

[58] "The Article 29 Working Party" was replaced by the European Data Protection Board (EDPB) on the 25th of May 2018. This is a group consisting of EU member state data protection authorities, who provide guidelines on how to interpret EU-regulation on data protection issues. Working Party 29"Guidelines on Consent under Regulation

users are pushed into giving consent to Location History in order to get access to Google Assistant, and to have photos sorted after location. There are also vague warnings about reduced functionality if the user disables Location History. These examples indicate that users who have been nudged into enabling Location History have not "freely given" their consent, and consequently it is not the valid consent required under the GDPR. If this is the case, the processing of this personal data may lack a valid legal basis.

5.1.2 Specific and informed?

In order to be considered valid, consent must be specific and informed. This means that the user must be presented with any information that is necessary to understand what he or she is consenting to, and that it should be clear what the consequences of giving consent could be.

When setting up a Google account, users are told that they can control how Google collects and uses their data. Users are also informed that they can adjust the settings and withdraw their consent. This shows that Google has provided information about rules, safeguards and rights. However, it is questionable whether the way that this information is presented is sufficient, considering users have to click "learn more" to get important information about the purposes of the processing, and the choices they have.

It is also questionable whether Google provides sufficient information about the purposes of the processing of location data. As shown in chapter 4, Google gives some information about processing personal data for advertising purposes, but only if the user clicks "learn more", and even then, this information is vague. Furthermore, phrasing such as "private map" can also mislead the user.

The relevant information regarding what Location History actually entails is hidden behind extra clicks and submenus, and the information about what the data is used for is ambiguous:

> *"Location History helps you get useful information (..) more useful ads on and off Google"*

Even if the consumer finds and reads the information under "Learn more", many users will probably not understand to what extent their location data is processed, that it is stored indefinitely, and how it is used for advertising

2016/679" p. 7 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

purposes. In particular, when using a service such as Google Assistant or photos grouped by location, it may not be obvious for the user that location data is being collected and stored, or for what purposes. This may be at odds with the notion of a "specific and informed" consent.

5.1.3 Unambiguous?

In order for consent to be valid, the user must have given an "unambiguous indication" through a "clear and affirmative action", that he or she consents to Google processing his or her personal data for advertising purposes through Location History.

In this context, it is worth mentioning that if Google was to base the processing of personal data in Web & App Activity on consent, and not legitimate interest (as we anticipate), consent would not be considered "unambiguous" since Web & App Activity is turned on by default. Pre-ticked boxes and "blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data."[59]

Google claims that the user must opt in before it can process location data collected through "Location history". However, since this consent is given after the user has been exposed to dark patterns such as deceptive click-flows and hidden information, it is questionable whether the data subject has given an "unambiguous indication". Furthermore, this raises questions about whether the consent is "obvious". As demonstrated, the user may also have declined to turn on Location History several times, but will continue to be nudged toward turning it on in different contexts.

The user has to perform extra actions, such as clicking "Learn more", to get information about the purpose of the processing of the personal data. The presentation of this information is ambiguous, and consequently may not be in accordance with the requirements for an "unambiguous consent".[60]

[59] Working Party 29"Guidelines on Consent under Regulation 2016/679" p. 16
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
[60] Working Party 29"Guidelines on Consent under Regulation 2016/679" p. 17
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

5.2 Legitimate interests

Processing of personal data may in certain circumstances be based on the data controller's legitimate interests.[61]

According to Google's privacy policy:

> *"We process your information for our legitimate interests and those of third parties while applying appropriate safeguards that protect your privacy. This means that we process your information for things like: […] Providing advertising to make many of our services freely available for users"* [62]

Since data collected through Web & App Activity is used for advertising purposes, and the setting is opt-out, it seems reasonable to assume that Google is relying on legitimate interest as the legal grounds for processing this data.

Under the GDPR, the processing of personal data is lawful if it is "necessary for the purposes of the legitimate interests of the controller".[63] However, if a data controller (in this case Google) is relying on legitimate interests for processing personal data, this must be balanced against the interest or fundamental rights and interests of the data subject. A legitimate interest must also be "lawful", "sufficiently clearly articulated" (transparent) and "represent a real and present interest".[64]

5.2.1 Transparency

As demonstrated in chapter 4, the information provided about the purposes and extent of data collection through Web & App Activity is not particularly clear. The fact that location data is collected as a part of this setting is hidden behind extra clicks, and information stating that this data may be used for advertising is only available under limited circumstances. Additionally, the fact that Web & App Activity is enabled by default is hidden when setting up a Google account.

---

[61] GDPR art. 6(1)(f)

[62] "Google Privacy Policy" https://policies.google.com/privacy#enforcement

[63] GDPR Art. 6(1)(f)

[64] Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" p. 25 and p. 52 www.dataprotection.ro/servlet/ViewDocument?id=1086

Furthermore, in the limited contexts where Google actually provides information about this data being used for advertising, the description of how the data is used is ambiguous:

> *"This data helps Google give you more personalised experiences across Google services, such as faster searches, better recommendations, and useful ads, both off and on Google"*

This phrasing seems like a blanket disclaimer that permits a wide range of purposes for using data collected through Web & App Activity.

Consequently, as the purposes for the collection and use of personal data from Web & App Activity are, in our opinion, unclear, this does not seem to fulfil the requirement for legitimate interest as a legal basis.

5.2.2 Balancing test

In order for legitimate interest to be a valid legal ground for processing personal data, it must be considered whether Google has a legitimate interest that overrides the individual's interests, rights and/or freedoms. This balancing test must be carried out by the data controller.[65]

Several features must be taken into account when performing a balancing test: The nature of the interests of the controller, the possible prejudice suffered by the controller, the nature of the data, the status of the data subject, and the way that data is processed. Additionally, the data controller must take into account the fundamental rights and/ or interests of the data subject that could be impacted.[66]

Privacy and the right to protection of personal data is a fundamental right in the EU.[67] Therefore, there is a high barrier to set aside the individual's rights and interests in privacy matters.

As mentioned, Google states in its privacy policy that it has a legitimate interest to provide "advertising to make many of our services freely available for

[65] GDPR art. 6 (1)(f) GDPR and recital 47.
[66] Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" p. 55 www.dataprotection.ro/servlet/ViewDocument?id=1086
[67] Art. 8(1) of the Charter of Fundamental Rights of the European Union, art. 16(1) of the treaty on the Functioning of the European Union (TFEU), art. 1(2) and recital 1 GDPR.

users".[68] However, the extensive tracking performed through features such as Web & App Activity and Location History is very invasive, especially considering that the tracking happens regardless of user interaction, and that the collected data is retained on a seemingly indefinite basis. As a result, Web & App Activity and Location History are arguably privacy adverse. Any legitimate interest to provide advertising should therefore arguably be overridden by the data subject's fundamental right to privacy.

5.2.2.1 Reasonable expectations

In order for a legitimate interest to be valid, it must be considered whether the data subject had "reasonable expectations" at the time and in the context of the collection of personal data, that the personal data could be used for advertising and marketing purposes.[69] This consideration should be based on an objective perspective of what a reasonable person could expect.

It is questionable whether the users had a "reasonable expectation" to believe that Google is tracking their location for marketing purposes in the context of Web & App Activity. In many cases, Google will have been collecting this information since users created a Google account. Today, a number of consumers may be aware of such processing due to the media and consumer organisations contributing to more information and awareness of these practices. Additionally, as shown, Google provides some information to the user.

However, many consumers may not have been aware of this processing when they first created the account. In these cases, the data subject would not have had reasonable expectation for such processing of personal data at the time when Google started collecting the data. Similarly, users who (with or without intent) have enabled Location History, may not have been aware of the extent of tracking and use of the data.

One must also consider whether the context of the collection could give the data subjects reasonable expectations that their location data would be used for advertising purposes. As outlined throughout this report, the extent of the collection of personal data for advertising purposes is under-communicated and hidden in the presentation of both Location History and Web & App activity.

This indicates that many users would not have reasonable expectations about Google processing their personal data for advertising purposes. In addition,

[68] "Google Privacy Policy" https://policies.google.com/privacy#enforcement

[69] GDPR art. 6 (1)(f) and recital 47

since Web & App activity is turned on by default, the data subject would likely not have seen any information about location data being collected, and could therefore probably not have reasonable expectations for such processing, and at such a comprehensive scale.

The Article 29 Working Party recommend that data controllers demonstrate the reasons why they consider their own interest to override the data subject's interests and rights. This should be demonstrated in a clear and user-friendly way. The burden of proof is with the data controller.[70] *In situations where the data subject does not have reasonable expectations of the processing of personal data, this will imply that the data subject's interests and rights will override the controller's interests.*[71] *As the report has shown, Google collects personal data passively in the background and not necessarily while using the app.*[72] *With this in mind, it seems that the lack of a reasonable expectation at the time of collection would tip the balancing act in favour of the interest of the data subject.*

Safeguards

The implementation of certain safeguards can modify the legal grounds for processing personal data using legitimate interests. Such safeguards may include functions such as opting out of the processing of personal data, anonymisations of personal data, and particular transparency measures such as easy to use deletion tools.

Google claims to anonymise data. However, according to recent reports, this "anonymous data" can be easily re-identified as long as the user connects to their Google account.[73] In this case, anonymisation is not actually effective, and works against its purpose as a safeguard.

According to The Article 29 Working Party, "opt-in consent would almost always be required for [...] for tracking and profiling for purposes of direct marketing, behavioural advertisement, location-based advertising or tracking-based digital market research".[74] This implies that Google may lack a valid legal basis to process location data for marketing purposes through Web & App Activity.

---

[70] Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" p. 42 www.dataprotection.ro/servlet/ViewDocument?id=1086

[71] GDPR recital 47

[72] See this report, chapters 3.1 and 3.4.

[73] This is outlined in a 2018 report by researchers at the Vanderbilt University. "Google Data Collection" https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf

[74] Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" p. 47 www.dataprotection.ro/servlet/ViewDocument?id=1086

***

As we have seen, users are able to opt out of Web & App Activity by pausing the setting. However, it is unlikely that many users would ever opt out of Web & App activity, since they would likely not know that the setting is turned on by default. Furthermore, regular users will be unaware that location data is collected, that this data is used for advertising, or even that Web & App Activity exists in the first place.

In our opinion, because of the high barrier to protect the individual's right and interest in privacy matters, Google's interests does not override the data subject's interests and rights in this case.

5.3 Summary of legal analysis

As demonstrated throughout this chapter, the ways that Google has designed its Location History and Web & App Activity settings are problematic in light of European data protection requirements. In this report we have questioned the legal basis Google has for collecting and processing this location data.

It is questionable whether users have given free, specific, informed, and unambiguous consent to the collection and use of location data through Location History. It can also be discussed whether the user can withdraw his or her consent, since there is no real option to turn off Location History, only to pause it.

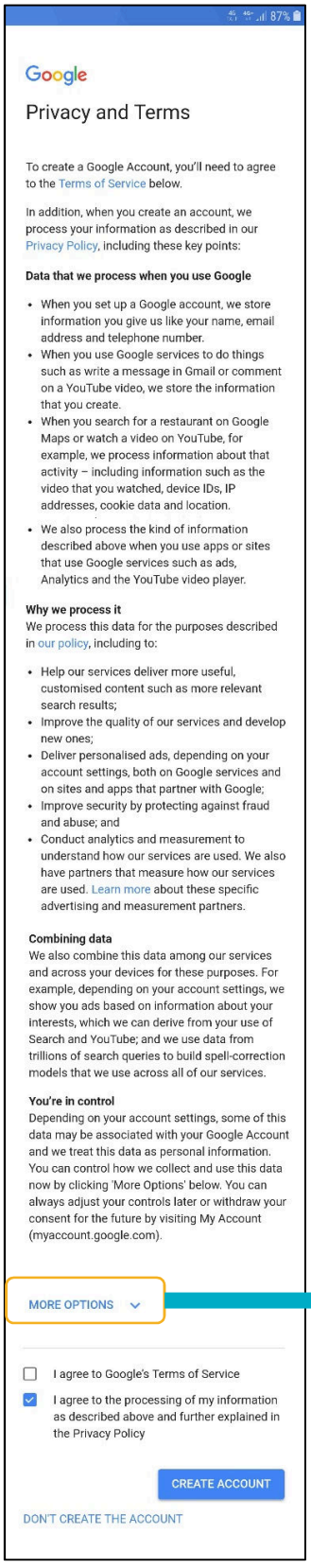
Since Web & App Activity is turned on by default, the collection and use of personal data through this setting cannot be based on consent. Google claims to have a legitimate interest in serving ads based on personal data, but the fact that location data is collected, and how it is used, is not clearly expressed to the user. This calls into question whether Google's legitimate interest in serving advertising as part of its business model, overrides the data subject's fundamental right to privacy. As we have argued above, in light of how Web & App Activity is presented to users, the interests of the data subject should take precedence in this case.

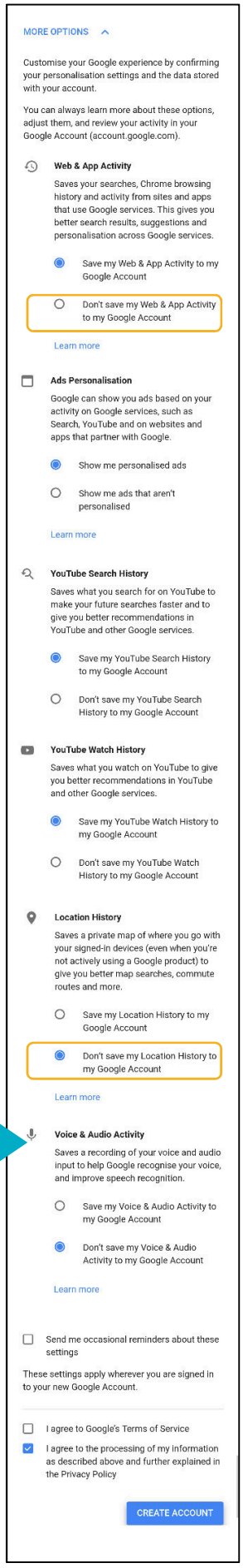


6 Appendix

Setting up a Google account.

The screenshots show what users are presented with when setting up an Android device. In order to see the different options, and to turn these on or off, users have to scroll through the truncated privacy policy, and click “More options”.





While disabling "Web & App Activity" will stop Google from storing location markers, it also prevents Google from storing information generated by searches and other activity. That can limit the effectiveness of the Google Assistant, the company's digital concierge.

Sean O'Brien, a Yale Privacy Lab researcher with whom the AP shared its findings, said it is "disingenuous" for Google to continuously record these locations even when users disable Location History. "To me, it's something people should know," he said.

[redacted] [redacted]: Aug 13 06:51PM -0700

I agree with the article. Location off should mean location off; not except for this case or that case.

The current UI *feels* like it is designed to make things possible, yet difficult enough that people won't figure it out. New exceptions, defaulted to on, silently appearing in settings menus you may never see is <redacted>.

The general concept of what I'd like to see on the location settings :

Location: On/Off (Off disables everything; On enables the ones selected items)
Enable GPS location (on/off)
Enable Bluetooth location (on/off)
Enable Bluetooth to report, even when Bluetooth is off (on/off)
Enable Web/App Activity (on/off)
Enable ... (on/off)

We already have this menu/style for non-Google apps.

This way the user can see and set, in ONE place all of the items related to location. If users find it useful for all of the bluetooth settings to be together, then have the "enable bluetooth to report location when bluetooth is off" in both menus.

Btw. Thank you whomever added the option for bluetooth to not respond to queries when bluetooth is off. (It used to respond, thereby giving location information away, even when location and bluetooth were off.)

On Mon, Aug 13, 2018 at 7:06 AM, [redacted]

wrote:

[redacted]>: Aug 14 12:03AM -0700

It is a bit complicated, and we might need better messaging.

There is a general location tracking for figuring out your home, work locations, and routines (you go to a cafe at the same time every week, then you might get a notification for that etc). This seems to run in the background all time.

But there is also a location information passed on with individual requests, like when you search for "Walmart", or ask for weather forecast. each app, search, news, home, etc seem to have a separate setting.

There is a valid use case. I might want to keep getting local results, while disabling always on location tracking. Or disable location in weather but keep it in news, etc.

On Monday, August 13, 2018 at 6:52:57 PM UTC-7, C[redacted] wrote:

[redacted]

Exhibit 19

From: [redacted]
To: [redacted]
Subject: [Industryinfo] Digest for [redacted] - 25 updates in 7 topics
Sent: Tue, 14 Aug 2018 17:43:51 +0000

[redacted] Google Groups

Topic digest

View all topics

- AP Exclusive: Google tracks your movements, like it or not - 11 Updates
- Musk Mulls Taking Tesla Private, Valuing Company at $82 Billion - 3 Updates
- "Google plans censored search engine for China" - The Intercept - 4 Updates
- [NY Times Op-Ed] A Better Way to Ban Alex Jones - 1 Update
- Brandon Downey: "Some thoughts on an Old Approach to China by Google." - 4 Updates
- Artificial intelligence 'did not miss a single urgent case' - 1 Update
- Google's censored Chinese search engine: a catalogue of ethical violations? - 1 Update

AP Exclusive: Google tracks your movements, like it or not

[redacted] Aug 14 10:01AM +0200

+1

[redacted] Aug 14 10:50AM +0200

There are three location-related settings on Android:

Location History: this controls whether your location is recorded in your timeline in Google Maps.

Location toggle on the device: simplifying a little, this controls whether GPS is enabled and can be found in the notification pulldown. If this is off, the phone will not attempt to determine its precise location. Most people never turn this off, since it will prevent Maps from telling you where you are.

Web and App Activity: a catch-all for recording search and Assistant query history. If you turn this off, you can't use Assistant.

The complaint in this article is that if you have Web and App Activity enabled and the location toggle enabled, then your search history entries contain your approximate location at the time you made the query. It's also not possible to remove them by clearing your location history, which is counter-intuitive - you have to clear your search history instead.

EXHIBIT NO. 19
P. Frederickson, CSR, CCR

[redacted] Aug 14 11:27AM +0200

Definitely confusing from a user point of view if we need googlers explain it to us :)

[redacted]

[image: Google Logo]

[redacted]

Google Cloud Platform UX
London, UK

[redacted]

On Tue, Aug 14, 2018 at 11:17 AM [redacted] wrote:

[redacted] Aug 14 12:45PM +0200

Although I know how it works and what the difference between "Location" and "Location History" is, I did not know Web and App activity had anything to do with location.

Also seems like we are not very good at explaining this to users.

Here is the screenshot from "My activity" setting:
https://screenshot.googleplex.com/s3AeEc4ZsEo

And When You click on Learn More:
https://screenshot.googleplex.com/qfNYTUS9h3C

cheers

[redacted]

--

. [redacted]*
. Publisher Solutions Consultant gPS
* . *Google Inc.

[redacted]

This email may be confidential and privileged. If you received this communication by mistake, please don't forward it to anyone else, please erase all copies and attachments, and please let me know that it has gone to the wrong person.The above terms reflect a potential business arrangement, are provided solely as a basis for further discussion, and are not intended to be and do not constitute a legally binding obligation. No legally binding obligations will be created, implied, or inferred until an agreement in final form is executed in writing by all parties involved.

This sample code is an experimental, unsupported Beta Feature (as such term is defined in the Google DoubleClick Platform Services Terms and Conditions, Advertising Platform Agreement, or Google Services Agreement related to AdX, that is in place between your company and the applicable Google entity that entered into such agreement, whichever is currently in effect (the "Agreement")). This sample code is hereby provided to you by the applicable Google entity that entered into the Agreement. It is provided for your convenience and is intended to model a possible solution.

On Tue, Aug 14, 2018 at 11:28 AM [redacted] wrote:

[redacted] Aug 14 08:26AM -0400

> Although I know how it works and what the difference between "Location" and "Location History" is, I did not know Web and App activity had anything to do with location.

> Also seems like we are not very good at explaining this to users.

Indeed we aren't very good at explaining this to users. Add me to the list of Googlers who didn't understand how this worked an was surprised when I read the article.

Of course, we shouldn't have to explain this to users. The real failure is that we shipped a UI that confuses users and requires explanation. We should redesign the UI so it's obvious what's

happening, and make it easy for users to choose the settings they want in one place without parsing complex details about product interactions.

[redacted]

[redacted] Aug 14 02:35PM +0200

Please don't comment!

[redacted] 14. Aug. 2018, 14:27:

[redacted] Aug 14 02:37PM +0200

Why?

[redacted] Aug 14 01:39PM +0100

[redacted]

REDACTED - PRIVILEGE

On Tue, Aug 14, 2018 at 1:26 PM [redacted] wrote:

[redacted] Aug 14 02:52PM +0200

In this case you can just as well demand switching industryinfo to readonly mode. People on the thread were extremely nice and careful in their statements and only meant to suggest a way to improve our services. This is [redacted]s useful in my opinion. But if the management believes that it generates more risk than reward, it should be made readonly. This would remove an important feedback mechanism, though.

[redacted] Aug 14 02:16PM +0100

[redacted]

REDACTED - PRIVILEGE

[redacted] Aug 14 10:36AM -0700

On Tue, Aug 14, 2018 at 1:50 AM, [redacted] wrote:

> contain your approximate location at the time you made the query. It's also
> not possible to remove them by clearing your location history, which is
> counter-intuitive - you have to clear your search history instead.

I believe the complaint of the article is that Google records location information when "Location" is off. The rest of the article is giving an example of the additional information gathered. It is not the primary complaint.

[I hope that commenting on the article proper is still acceptable.]

Back to top

Exhibit 20

From: [redacted]
To: [redacted]
Received: Tue, 14 Aug 2018 14:31:58 -0700
Subject: Re: AP Story on Location
Cc: [redacted]

[redacted]

REDACTED - PRIVILEGE

[redacted]

On Tue, Aug 14, 2018 at 12:17 PM [redacted] wrote:

REDACTED - PRIVILEGE

On Tue, Aug 14, 2018 at 8:45 AM [redacted] wrote:

[redacted]

REDACTED - PRIVILEGE

[redacted]

On Mon, Aug 13, 2018 at 12:53 PM [redacted] wrote:

REDACTED - PRIVILEGE

EXHIBIT NO. 20
P. Frederickson, CSR, CCR

On Mon, Aug 13, 2018 at 12:33 PM [redacted] wrote:

[redacted]

REDACTED - PRIVILEGE

[redacted]

On Mon, Aug 13, 2018 at 11:58 AM [redacted] wrote:

[redacted]

PRIVILEDGED & CONFIDENTAL

Hi [redacted]

[redacted]

REDACTED - PRIVILEGE

[redacted]

REDACTED - PRIVILEGE

On Mon, Aug 13, 2018 at 10:15 AM [redacted] wrote:

[redacted]

On Mon, Aug 13, 2018 at 9:38 AM [redacted] wrote:

> Good Morning [redacted]. I am back from vacation.
> Your name came up today during our Monday morning "Oh Shit" meeting in relation to this story.
> Both comms and policy are looking for an update on where we are in terms of fixing "location history" fixes and having one single place to turn off instead of 3:
>
> "There are a number of different ways that Google may use location to improve people's experience, including: Location History, Web and App Activity, and through device-level Location Services," a Google spokesperson said in a statement to the AP. "We provide clear descriptions of these tools, and robust controls so people can turn them on or off, and delete their histories at any time."
>
> Who should I reach out to for an update?

Thanks!

[redacted]

[redacted]

--

[redacted]

--

[redacted]

--

[redacted]

--
[redacted]
mail: [redacted]
visit: 1600 Amphitheater Parkway, Mountain View, CA 94043
call: [redacted]

Exhibit 24

Identity
UX Research

Impact of the AP Location History news coverage on Google users

Exploring user trust & trust related behavior

August 16, 2018 • [redacted]

Google | Proprietary & Confidential

IdAM

EXHIBIT NO. 24
P. Frederickson, CSR, CCR

Summary

- Sharp increase in visitors to products where users can adjust/monitor their privacy settings (Activity Controls) after AP news cycle started (8/13/2018)
- Nevertheless, the absolute # of users visiting Google privacy products was fairly small ([redacted] average [redacted])
- [redacted] increase in the proportion of users reporting "low trust" in Google amongst visitors of the Activity Controls page [redacted]
- [redacted]

ID UX Research

Section 01

Visits to trust related surfaces

My Account, My Activity, Google Takeout & [redacted]

My Account and other Google surfaces related to privacy contain trust signals

- Visit and action volumes on Google's privacy offerings are likely a proxy for user privacy concerns
- Some privacy related surfaces/products are:
  - Activity controls allows users to control [redacted] (e.g., Web & Apps Activity, Location History, ...)
  - Google Takeout allows users to download their data
  - My Activity allows users to review the data we collected about them
  - My Account - Large destination that either hosts or has prominent entry points to sections above. In addition to privacy settings, it also hosts security related information and other account settings (e.g. language settings)



Slide 4
---
1 For completeness [redacted]
[redacted], 8/17/2018

Activity Controls

ID UX Research



[redacted] increase in users visiting the Activity Controls page that hosts [redacted]

- The average # of visitors to My Account Activity Controls increased by about [redacted] since the AP report on 8/13
- The increase peaked [redacted]
- Over the past 3 days, about [redacted] users visited Activity Controls
- On 8/15 the visitor numbers strongly decreased, [redacted]

[redacted]

ID UX Research

[redacted] increase of users disabling at least 1[redacted] setting

- On 8/14, an [redacted]
- Despite the [redacted] increase[redacted], it's still only a very small proportion of [redacted]

[redacted]

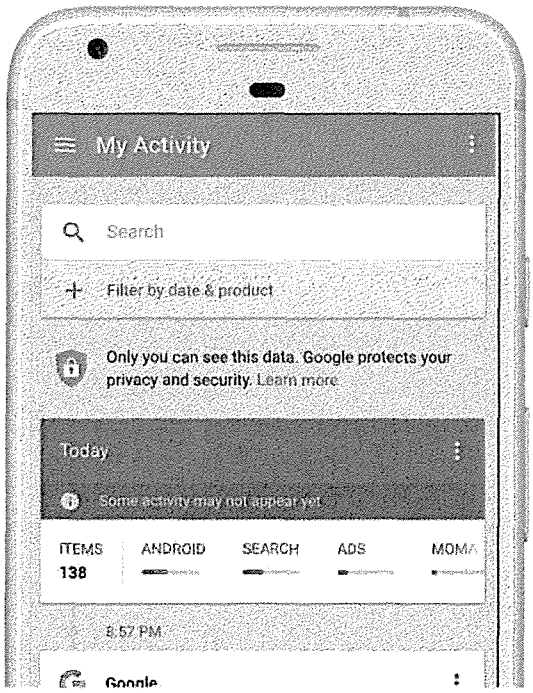
[redacted] disable increase [redacted]

- Location History and WAA setting was at the center of most news reports, thus [redacted]

[redacted]

ID UX Research

My Activity



ID UX Research

Given the [redacted], impact is less noticeable

- [redacted]
- [redacted], [redacted] increase [redacted] [redacted] compared to lower traffic [redacted]
- On average, slightly [redacted] [redacted] this proportion didn't [redacted] over the last 3 days

[redacted]

Section 02

User trust impact for Google Account visitors overall & Activity Controls visitors specifically

[redacted]

Strong drop in user trust sentiment [redacted]

- [redacted]
- Across My Account overall, [redacted] AP news led to a [redacted] increase [redacted]

I trust Google with my data

[redacted]

More info about in-product trust survey in appendix

Notes: [1] We define users a "low trust" if they strongly or somewhat disagree with the statement: "I trust Google with my personal data". [2] This change seems to be driven [redacted]

[redacted] Users with "low trust" are [redacted] more likely to [redacted]

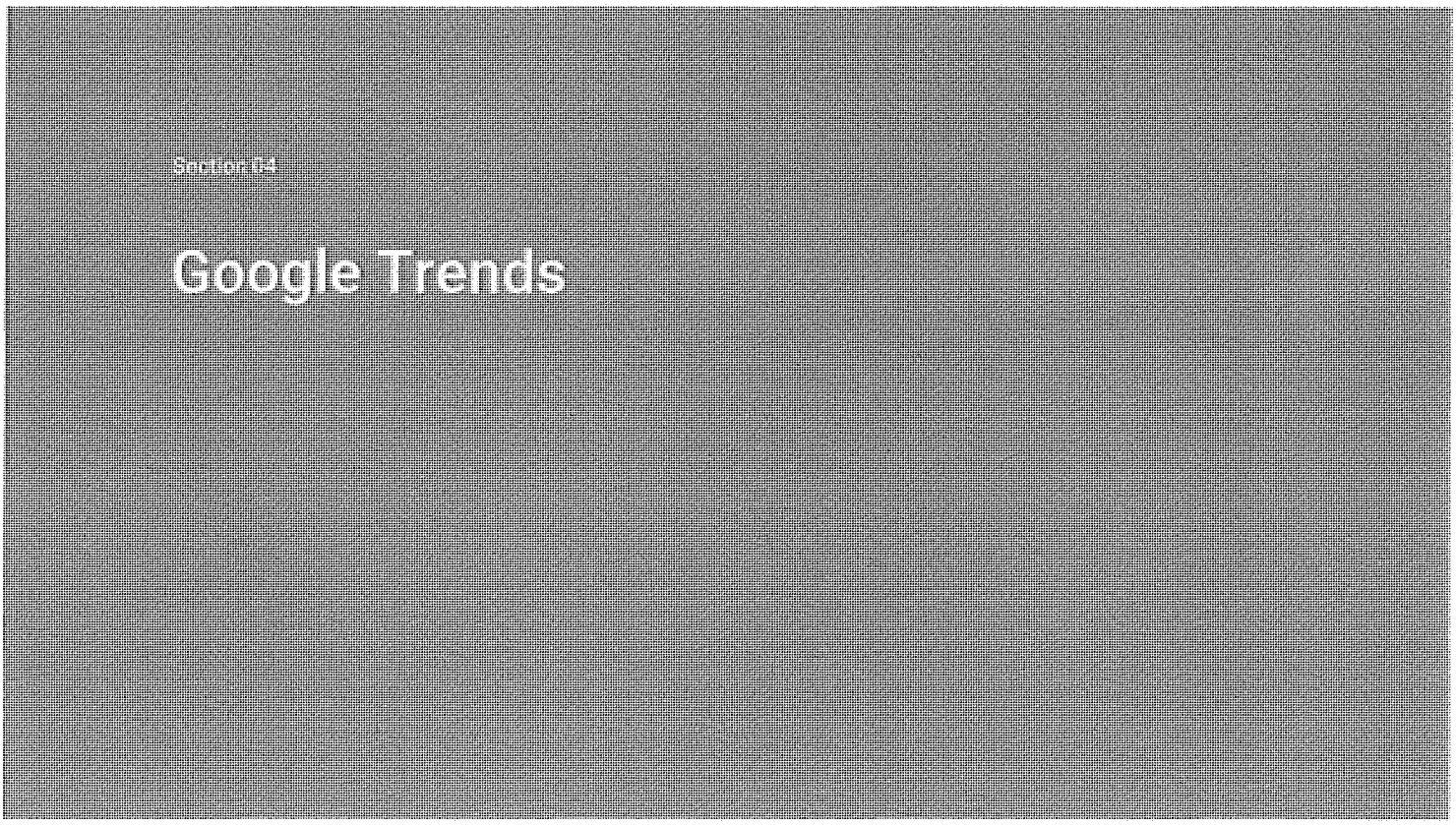
- Users who visit Activity Controls page and report "low trust" show a [redacted] increase in disabling at least [redacted]
- [redacted]

[redacted]

ID UX Research

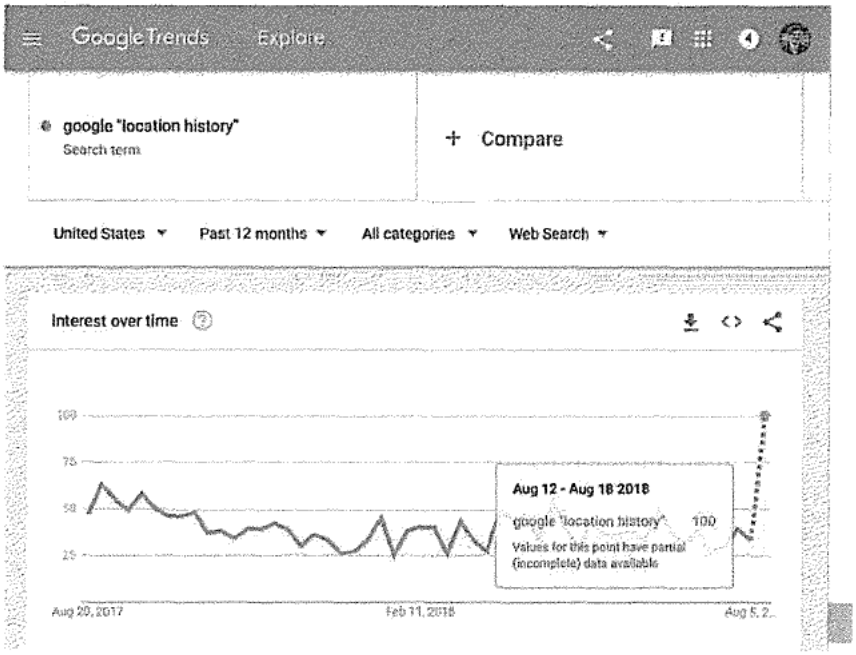

Section 03
Traffic from news article to Activity Controls



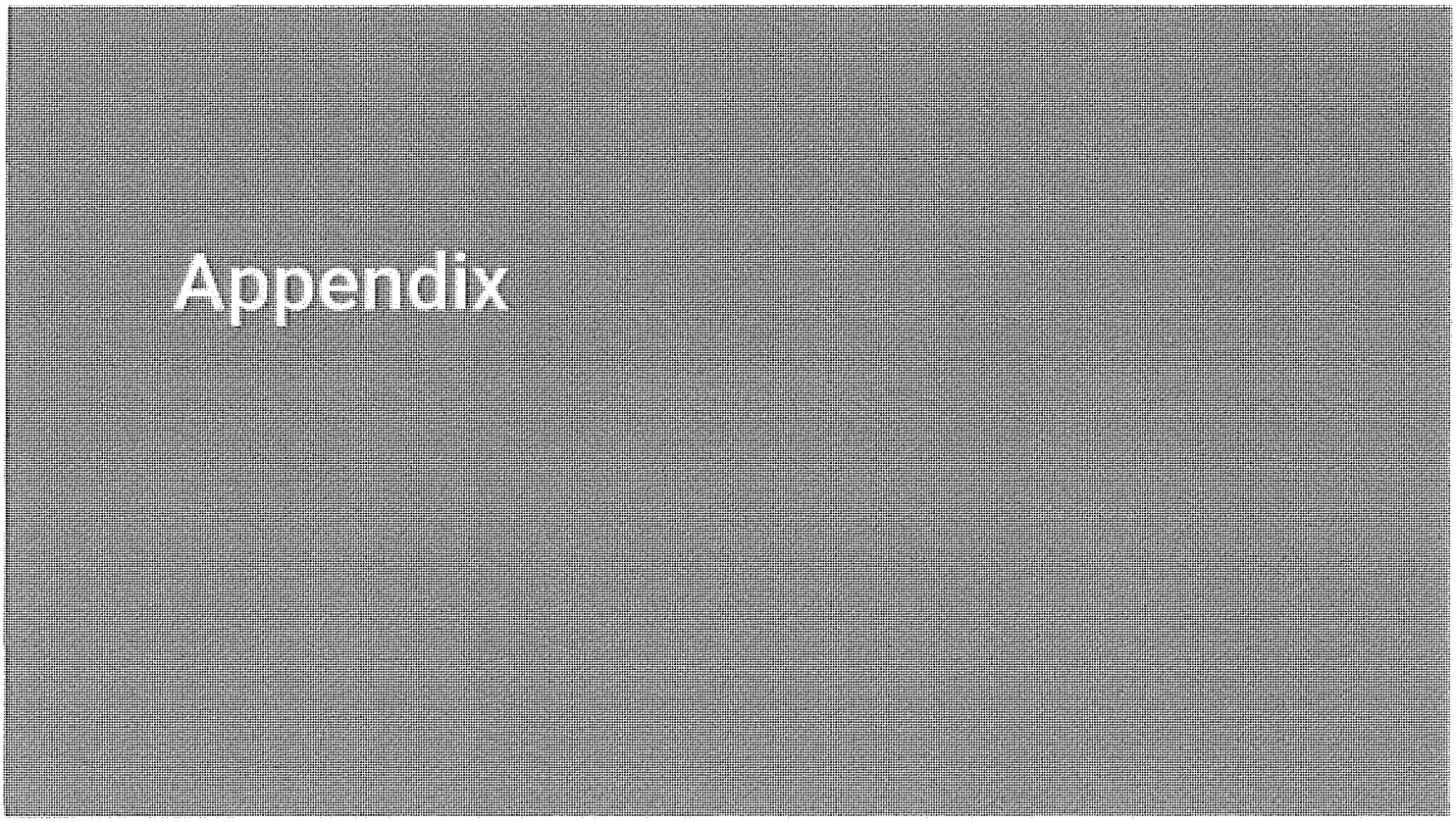

Sponsored
Google Trends

Strong increase for queries related to 'Google location history"

- Based on Google Trends, the search term" Google 'location history'" saw a significant increase



ID UX Research


Appendix

Trust & Privacy survey

- [redacted] we launched an [redacted] survey on [redacted] to track user sentiment related to privacy & trust [redacted]
- We track trust sentiment:
  - On pages [redacted])
  - On pages [redacted]
- 5 Agreement questions: *To what extent do you agree or disagree*:
  - [redacted]

[redacted]

Notes Summary:

Slide 19: [redacted]

[redacted]
REDACTED - PRIVILEGE

Exhibit 202

PERKINSCOIE

2901 North Central Avenue
Suite 2000
Phoenix, AZ 85012-2788

+1.602.351.8000
+1.602.648.7000
PerkinsCoie.com

February 21, 2020

Jean-Jacques Cabou
JCabou@perkinscoie.com
D. +1.602.351.8003
F. +1.602.648.7003

VIA E-MAIL BEAU.ROYSDEN@AZAG.GOV

Brunn (Beau) Roysden III
Chief, Appeals & Constitutional Litigation Division
Arizona Attorney General's Office
2005 North Central Avenue
Phoenix, AZ 85004

Re: Consolidated Final Responses to the First, Second, and Third Civil Investigative Demands

Dear Beau:

We write in further response to the Civil Investigative Demands (CIDs) by the Attorney General's Office (AGO). Below we provide a comprehensive document listing Google's final responses to the First, Second, and Third CIDs. This response represents several hundred hours of collective work by Google. Google believes that it fully satisfies its obligations with respect to the First, Second, and Third CIDs. To the extent the AGO disagrees, Google requests an in-person, meet-and-confer discussion in the very near future, perhaps in conjunction with one of the several upcoming EUOs at which we will be together.

This letter is not intended to and does not waive any applicable privileges or protections, including any attorney-client, work product, or other privileges or constitutional protections. Should any privilege or protection apply to the information provided to you, such disclosure was inadvertent and was not intended to constitute a waiver of such privilege or protection. In such an instance, we respectfully request the return of such material to our firm pursuant to our agreement. By responding here, or otherwise, Google does not waive any of its objections, and Google specifically reserves its right to raise, at any time, any substantive or procedural objections it may have.

Finally, we also request that this response, and all correspondence regarding the CIDs, be afforded confidential status pursuant to the Confidentiality Agreement in this matter, the Consumer Fraud Act, A.R.S. § 44-1525 et seq., and the Arizona Public Records Law, A.R.S. § 39-121 et seq.

Sincerely,

CONFIDENTIAL
147291338.1



Jean-Jacques Cabou
JC:jm

INTRODUCTION AND RESERVATION OF RIGHTS

Google provides the below responses and information to respond to the discovery demands by the AGO and its outside counsel. As stated previously, including in Google's August 26, 2019 letter, if, notwithstanding Google's efforts to comply with the AGO's discovery demands, an enforcement petition or judicial complaint of any kind is brought against Google, it reserves the right to assert any claim, defense, or argument it may have.

GOOGLE'S RESPONSES TO THE FIRST CID

I. DEMANDS FOR INFORMATION

Demands for Information Regarding User Location Tracking

DEMAND FOR INFORMATION NO. 1
Explain the types of data Google collects from which a user's location can be determined.

INITIAL RESPONSE (April 17, 2019): The user location information that Google may collect depends on a number of factors. As Google explains in its Privacy Policy (available at https://policies.google.com/privacy#infocollect), user location information includes information from inputs such as search queries and other information the user chooses to provide to Google (e.g., destination address for driving directions), users' IP addresses, device sensors (as explained further below in Response to DFI No. 2), and device signals including GPS, information cellular networks provide to a device, information from nearby Wi-Fi networks, and information from nearby Bluetooth devices. Location information can be used to provide a range of functionality, including ensuring that Google products and services use the correct default language based on a user's location, providing search results that relate to a relevant place, or providing optional account features, such as current traffic predictions.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 2
Explain how user location data is collected in connection with Android, Google-authored apps, Google search through a web browser, and Google Accounts.

INITIAL RESPONSE (April 17, 2019): As we explain in our Privacy Policy and above in response to Demand for Information No. 1, the user location information that Google collects depends on a number of factors, including the product or service being used and an individual user's settings. As described in Google's Privacy Policy and public documentation, when users interact with Google products and services, including when certain Google Account features and settings are enabled, location information may be collected. Further, this location information may be characterized as providing implicit or explicit information about a user's location.

Implicit user location information does not tell Google where a user's device is located, but through user inputs, Google may infer that a user is either interested in a place or that the user might be at a place. An example of implicit user location information would be a user inputting a search query for a particular place. For example, if a user conducts a Google Search for "Eiffel Tower" Google may infer that the user may like to see information for places near Paris, and Google can then use that inference to provide localized recommendations about those places.

When users use or interact with certain Google products and services, their devices may send explicit user location information to enable Google to provide those products and services. Explicit user location information contains information about where a device is located and comprises the location information types described below. Some Google products and services, such as turn-by-turn navigation in Google Maps for mobile, require explicit device location. For these products and services, users must turn on device-based settings that can be used to derive precise location.

The source and nature of the explicit user location types that Google collects are described below as well as in the Google Privacy Policy:

- **GPS**

GPS is a radio navigation system that is relatively precise. It works by using radio waves between satellites and a receiver inside a device to geolocate the device. The device's GPS receiver uses data from the satellite signals to triangulate where the device is and what time it is.

- **Device sensors**

Built-in sensors on devices measure motion, orientation, and various environmental conditions. The Android OS supports a number of these different sensor types, which vary from device to device. These sensors are used to provide a variety of functionality to Android OS developers—such as the ability to measure device movement or positioning to support motion-based games, or to report a compass bearing for a travel application.

Android OS application developers, including Google, can use accelerometers, gravity sensors, gyroscopes, rotational vector sensors, barometers, orientation sensors, and magnetometers to more precisely determine a device's location. For example, Google uses the accelerometer readings to help determine the device's orientation and direction, the gyrometer helps determine if a user is turning, and the barometer can help determine the user's elevation.

- **Cellular Network Information**

Depending on the type of network to which the device is connected, Google may collect the tower-broadcasted latitude and longitude of the cell tower from which the device is receiving service.

- **Wi-Fi & Bluetooth Scanning**

These settings (on a user's device) allow apps and services to scan for publicly available information from nearby devices (for example, Wi-Fi access points or Bluetooth beacons). These settings allow the user's device to scan for nearby networks or other devices, even when Wi-Fi or Bluetooth connectivity settings are disabled on a user's device.

- **IP Address**

IP address information is another type of information that Google collects, stores, and uses, as explained in Google's Privacy Policy. IP addresses are required for devices to be able to connect to one another through the Internet and are necessary for online services to function. Because IP addresses are usually assigned in geographic blocks, they may be used to provide an estimate of the location from which a device is connecting to the Internet. Inferring location based on an IP address alone can be quite inaccurate. Nonetheless, Google may use IP addresses when other more precise location information may be unavailable or in connection with available user location information.

Google may need to roughly estimate a user's location by using an IP address, even when particular device and Google Account settings affecting other user location information are disabled. For example, it is important for Google to approximate the location of its users to comply with certain legal requirements, such as restrictions on advertising for gambling services, which differ by jurisdiction. Google may also collect, store, and use user location information to help detect fraud or other suspicious activity on a user's account. For example, IP address information may enable users to determine when their Google Accounts have been compromised by unusual activity. Users can review the dates and times on which their Google Accounts have been accessed, as well as the IP address and general location from which these accesses occurred.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it, including in answering DFI No. 7, below. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
In Google's February 28, 2019 letter to the AGO and in its first response to the First CID, Google objected to requests to the extent that they were overly broad and unduly burdensome in defining a Relevant Time Period of more than 10 years—January 1, 2007 - present—across such a broad range of products and services. Google explained that in the absence of appropriate limitations, the scope was not manageable and made it difficult for Google to provide useful information in a timely and efficient manner. Subject to and without waiving those objections, Google provided detailed and substantive narrative responses and produced documents.

Additionally, Google made three witnesses available for examinations under oath, who were prepared to speak about how user location information is collected in connection with Android and Google

Accounts. Further, as we mutually agreed, Google is making a fourth witness available for examination under oath later this month to speak about how user location information is collected in connection with Google-authored apps and Google search through a web browser.

Furthermore, in its April 17, 2019 response, Google comprehensively answered how it collects location information. In response to Demand for Information No. 2, Google described GPS, device sensors, IP Addresses and scanning for Wi-Fi, Bluetooth, and cellular network information. Moreover, in its response to Demand for Information No. 7, Google provided additional explanations about location information collection via Google Account (including Location History, Web & App Activity, and Google Location Sharing) and device settings, including the Device Location Setting, Google Location Accuracy (formerly known as Google Location Services), and Usage & Diagnostics. Google also explained that the user location information that Google collects depends on a number of factors, including the product or service being used and an individual user's settings. In its June 20, 2019 supplemental response, Google asserted that "it ha[d] fully responded" and said "[i]f there are follow-up questions regarding this response" to "please let us know."

Your January 17, 2020 letter says that "Google's response does not mention products that the AGO now knows are involved in user location data collection, such as the FLP (Fused Location Provider) or ULR (User Location Reporting). *See, e.g.*, [redacted] EUO Tr. at 66:1–8; [redacted] EUO Tr. at 68:11–69:18." Your letter reflects a misunderstanding of relevant facts. First, Fused Location Provider does not collect location information. It "can provide estimated location received from Google Location Services." *See, e.g.*, [redacted] EUO Tr. at 60:21–23. Google described Google Location Services (now known as Google Location Accuracy) in its written responses, including as early as April 17, 2019. Second, User Location Reporting is tied to the Google Location History Product, which Google described in multiple Demands for Information, including, for example, Demands No. 4–8, 11, 12, 15, 17, and 18. Google specifically explained in its responses, including on April 17 and September 4, 2019, that "users can also opt out a particular device from collecting and reporting user location to Location History."

DEMAND FOR INFORMATION NO. 3
Describe the user location data collected in connection with Android, Google-authored apps, Google search through a web browser, and Google Accounts, including the precision of the data and the frequency with which the data is collected.

INITIAL RESPONSE (April 17, 2019): We describe the location information that Google collects in response to Demand for Information No. 2 above. The frequency with which location information is collected depends on a number of factors, including how often the user is interacting with Google products and services, the product or service being used, and an individual user's settings. For example, if Web & App Activity is enabled for a user's Account, the frequency of collection will

depend on the user's web activity or other interactions with Google products and services (e.g., finding a place in Maps).

The degree of precision of location information is also described in response to Demand for Information No. 2. As we explain above, user location inputs may be characterized as providing implicit or explicit information about a user's location. Implicit user location information does not tell Google where a user's device is located, but through user input allows Google to infer that a user is either interested in a place or that the user might be at a place. Explicit user location information contains information about where a device is located, and enables Google to provide its products and services to users.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
In Google's February 28, 2019 letter to the AGO and in its first response to the First CID, Google objected to requests to the extent that they were overly broad and unduly burdensome in defining a Relevant Time Period of more than 10 years—January 1, 2007 - present—across such a broad range of products and services. Google explained that in the absence of appropriate limitations, the scope was not manageable and made it difficult for Google to provide useful information in a timely and efficient manner. Subject to and without waiving those objections, Google provided detailed and substantive narrative responses and produced documents.

Specifically, Google's April 17, 2019 response to this Demand explained that Google described the degree of precision of location information in response to Demand for Information No. 2. There, Google addressed precision of GPS, IP Address, device sensors, implicit location information, and Google Maps location information.

Google also produced multiple informative documents on the topic of the precision of location information. For example:

- GOOG-GLAZ-00044520 - GOOG-GLAZ-00044770: Discusses the precision of numerous kinds of information from inputs including Wi-Fi, GPS, Compass, and magnetometers.
- GOOG-GLAZ-00173091 - GOOG-GLAZ-00173105: Discusses the precision of location in the context of indoor navigation.
- GOOG-GLAZ-00171989 - GOOG-GLAZ-00171995: Discusses the precision of location in the context of indoor navigation.
- GOOG-GLAZ-00171906 - GOOG-GLAZ-00171908: Discusses the coarsening of location across Google and the [redacted]

- GOOG-GLAZ-00090592 - GOOG-GLAZ-00090600: Discusses [redacted] in logging" and its application.
- GOOG-GLAZ-00159799 - GOOG-GLAZ-00159801: Discusses coarsening non-device location in search.
- GOOG-GLAZ-00141961 - GOOG-GLAZ-00141986: User Location Newsletter.
- GOOG-GLAZ-00096793 - GOOG-GLAZ-00096823: Entitled "Precise IP."

Additionally, Google made three witnesses available for examinations under oath, who were prepared to speak about the user location information collected in connection with Android and Google Accounts, including the precision of the information and the frequency with which the information is collected. Further, as we mutually agreed, Google is making a fourth witness available for examination under oath later this month to speak about the user location information collected in connection with Google-authored apps and Google search through a web browser, including the precision of the information and the frequency with which the information is collected.

Your January 17, 2020 letter alleges that "Google's 6/20/2019 response is devoid of any substantive information." As an example, you cite the topic of changes to the precision of WAA location information in 2014/2015 or early 2019. See [redacted] EUO Tr. at 185:19–187:11, 193:10–194:19, 195:11–19, 197:25–204:22. Your citation to Google's testimony is proof that Google made knowledgeable witnesses available on the topic. Further, on September 4, 2019, Google responded to all of the AGO's Demands for Information and Requests for Production on this topic. Google's responses and productions specifically addressed the topics of the storage of device-based location as part of Web & App Activity in 2014/2015, and its 2019 changes to coarsen Web & App Activity location information. This includes Google's production of relevant launch reports and other documents in response to Requests for Production No. 7 and 18 and Google's written responses to Demands for Information No. 22, 23, and 25 in the AGO's Third CID.

Furthermore, for example, for Web & App Activity before 2015, device location was coarsened to approximately a neighborhood-sized area with a sufficient number of unique users (e.g., 1,000). When precise location was added in 2015, the location provided by the user's device was stored, which could be a precise lat/lon. In 2019, the device-based Web & App Activity location was moved to a coarser level than it was in 2015, approximately a city-sized area with a sufficient number of unique users (e.g., +1,000).

DEMAND FOR INFORMATION NO. 4
Explain how Google stores and deletes user location data collected in connection with Android, Google-authored apps, Google search through a web browser, and Google Accounts, including the length and location of storage.

INITIAL RESPONSE (April 17, 2019): As Google explains in its Privacy Policy and above in response to Demands for Information Nos. 1-3, the way that Google collects, stores, and deletes user location information depends on a number of factors, including the product or service being used and an individual user's settings. For example, users can change their device location settings in the "Security and location" section of their Pixel. In their Google Account, users can remove Location History entries from their Timeline and Web & App Activity entries from their My Activity page at any time (available at https://myaccount.google.com/activitycontrols).

As Google explains on its Data Retention page (available at https://policies.google.com/technologies/retention), as a general matter, when a user deletes data in the user's Google Account, Google starts the process of removing it from the product and its systems. Google also tries to ensure that its products and services protect information from accidental or malicious deletion, including of user location information. Because of this, there may be delays between when users delete something and when copies are deleted from Google's active and backup servers. Google products and services also use encrypted backup storage as another layer of protection to help recover from potential disasters. Data can remain on these systems for up to six months.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
In Google's February 28, 2019 letter to the AGO and in its first response to the First CID, Google objected to requests to the extent that they were overly broad and unduly burdensome in defining a Relevant Time Period of more than 10 years—January 1, 2007 - present—across such a broad range of products and services. Google explained that in the absence of appropriate limitations, the scope was not manageable and made it difficult for Google to provide useful information in a timely and efficient manner. Subject to and without waiving those objections, Google provided detailed and substantive narrative responses and produced documents.

In addition to explaining Google's general policies about data deletion, Google's April 17, 2019 response also explained that users could view, manage, and delete their Location History and Web & App Activity data at any time.

Additionally, Google made three witnesses available for examinations under oath, who were prepared to speak about how Google stores and deletes user location information collected in connection with Android and Google Accounts, including the length and location of storage. Further, as we mutually agreed, Google is making a fourth witness available for examination under oath later this month to speak about how Google stores and deletes user location information collected in connection with Google-authored apps and Google search through a web browser, including the length and location of storage.

Again, because of the overbroad scope of this DFI, it is difficult for Google to provide useful information. But subject to and without waiving its objections, Google stores and deletes user location information including but not limited to as follows:

Store	Data Stored	Retention/Deletion[1]
SensorVault/Location History	Location information for users that have enabled Location History.	Deleted upon user request and/or account closure.
Web & App Activity	Coarse location information from which a user used a Google service.	Deleted upon user request and/or account closure.
[redacted]	Cache of recent user location, coarse or precise depending upon account/device settings.	Deleted upon user request and/or account closure or, if neither of those occurs, within two months of collection.
Google Location Accuracy and Google Location Services	Location information for users with Google Location Accuracy/ Google Location Services on - not tied with user's account.	[redacted]

Google also produced multiple informative documents on the topic of the length and location of storage of location information. For example,

- GOOG-GLAZ-00176439 - GOOG-GLAZ-00176441: Discusses the length of data storage.
- GOOG-GLAZ-00175307 - GOOG-GLAZ-00175312: Discusses the length of data storage in the specific context of advertising.
- GOOG-GLAZ-00093216 - GOOG-GLAZ-00093244: Discusses SensorVault.
- GOOG-GLAZ-00168023 - GOOG-GLAZ-00168032: Discusses specific retention for different data types.
- GOOG-GLAZ-00167051 - GOOG-GLAZ-00167056: Discusses various locations in which data is stored.

[1] The information provided in this column is also subject to Google's Privacy and Data Retention Policy, available at https://policies.google.com/technologies/retention.

- GOOG-GLAZ-00082159 - GOOG-GLAZ-00082160: Discusses "LH retention storyline."
- GOOG-GLAZ-00154824 - GOOG-GLAZ-00154826: Discusses Writing Location History Setting.
- GOOG-GLAZ-00151237 - GOOG-GLAZ-00151247: Discusses SensorVault storage requirements and retentions.
- GOOG-GLAZ-00196328 - GOOG-GLAZ-00196330: Discusses "retention plans."

Moreover, in response to more detailed questions about user location information deletion and storage in the AGO's Third CID, Google provided additional narrative information. For example, in response to Demand for Information No. 10, which asked more specifically about deletion of user location information outside of Location History and Web & App Activity, Google provided relevant information for all of its Google Mobile Services products:

- Google
- Chrome Browser
- Gmail
- Google Maps
- YouTube
- Google Play Store
- Drive
- Google Play Music
- Google Play Movies
- Duo
- Google Photos

Google also provided additional information about the storage and deletion of user location information in relation to Location History and Web & App Activity in its response to the Third CID. Specifically, Google explained that it introduced a feature in May of 2019 that allows users to set the information to auto-delete after 3 or 18 months, or to be retained indefinitely for users to manage and delete when they wish.

Furthermore, the AGO's Fourth CID asks additional questions about how and under what circumstances Google stores and deletes user location information (for example, in Demands for Information No. 1, 4, 12, and 13), which Google is in the process of responding to.

Finally, the specific example your January 17 letter cites from documents Bates-stamped GOOG-GLAZ-00031110 simply elaborates on information Google already provided. As Google explained in its original response to this Demand, "as a general matter, when a user deletes data in the user's Google

Account, Google starts the process of removing it from the product and its systems. Google also tries to ensure that its products and services protect information from accidental or malicious deletion, including of user location information. Because of this, there may be delays between when users delete something and when copies are deleted from Google's active and backup servers."

DEMAND FOR INFORMATION NO. 5
Explain how Google uses user location data collected in connection with Android, Google-authored apps, Google search through a web browser, and Google Accounts.

INITIAL RESPONSE (April 17, 2019): Google's Privacy Policy and user instructional videos describe the information that Google collects, why it collects that information, and how Google keeps that information secure. The Privacy Policy specifically explains to users how Google uses location information in a section entitled, "Information Google collects," with a subsection titled, "Your location information." Under Google's Terms of Service and Privacy Policy, users agree that Google can collect information about location. As Google's Privacy Policy states, we "collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you."

As we explain in our response above to Demand for Information No. 2, and in our Location Data page (available at https://policies.google.com/technologies/location-data), user location inputs may be characterized as providing implicit or explicit information about a user's location. Implicit user location information does not tell Google where a user's device is located, but through user inputs, allows Google to infer that a user is either interested in a place or that the user might be at a place. Explicit user location information contains information about where a device is located, and enables Google to provide its products and services to users.

Google also uses user location information collected when Location History and Web & App Activity are enabled to provide advertising services to signed-in users. Google does not use information from Location History and Web & App Activity if a signed-in user has opted out of ads personalization features. When Location History and Web & App Activity are disabled, they do not provide user location information to Google.

Additionally, Google uses location information from users who have enabled Location History to report aggregated and anonymised statistics to advertisers—for example, aggregate number of store visit conversions. Store visit reports provide advertisers with only anonymized and aggregated statistics about how ad clicks and viewable impressions are followed by visits to stores, and cannot be tied to individual ad clicks, viewable impressions, or individuals.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
In Google's February 28, 2019 letter to the AGO and in its first response to the First CID, Google objected to requests to the extent that they were overly broad and unduly burdensome in defining a Relevant Time Period of more than 10 years—January 1, 2007 - present—across such a broad range of products and services. Google explained that in the absence of appropriate limitations, the scope was not manageable and made it difficult for Google to provide useful information in a timely and efficient manner. Subject to and without waiving those objections, Google provided detailed and substantive narrative responses and produced documents.

Google made three witnesses available for examinations under oath, who were prepared to speak about how Google uses user location information collected in connection with Android and Google Accounts. Further, as we mutually agreed, Google is making a fourth witness available for examination under oath later this month to speak about how Google uses user location information collected in connection with Google-authored apps and Google search through a web browser.

Your January 17 letter asks about [redacted]. Google produced multiple documents on [redacted] and [redacted] each of which are proprietary technologies important to Google's location-related work, including:

- GOOG-GLAZ-00173493 - GOOG-GLAZ-00173503: Describing, among other things, Google's work "to build platforms that allow other teams within Google to leverage [redacted] data."
- GOOG-GLAZ-00168730 - GOOG-GLAZ-00168818: Describes uses of [redacted] data.
- GOOG-GLAZ-00168710 - GOOG-GLAZ-00168714: Describes uses of [redacted] data.
- GOOG-GLAZ-00022990 - GOOG-GLAZ-00022990: Discussing "raw location clients."
- GOOG-GLAZ-00167051 - GOOG-GLAZ-00167056: Discussing integration of [redacted] location signals.
- GOOG-GLAZ-00082055 - GOOG-GLAZ-00082059: Discussing GoogleFit and PlaceVault.
- GOOG-GLAZ-00153420 - GOOG-GLAZ-00153423: Discussing the "upcoming launch of [redacted]"
- GOOG-GLAZ-00077279 - GOOG-GLAZ-00077355: Describing Timeline and the History of Timeline, including its data sources and other particulars.
- GOOG-GLAZ-00034858 - GOOG-GLAZ-00034946: Discussing the "Location Platform Summit- Welcome."
- GOOG-GLAZ-00141961 - GOOG-GLAZ-00141986: User Location Newsletter.
- GOOG-GLAZ-00162682 - GOOG-GLAZ-00163027: Geo June 2017 "[redacted] Review."
- GOOG-GLAZ-00147911 - GOOG-GLAZ-00147946: [redacted] Ads Targeting Slides.

Moreover, Google is in the process of responding to your Fourth CID, which specifically asks about [redacted] in Demand for Information No. 12.

DEMAND FOR INFORMATION NO. 6
Explain the disclosure to third parties of user location data collected in connection with Android, Google-authored apps, Google search through a web browser, and Google Accounts.

INITIAL RESPONSE (April 17, 2019): As described in our General Objections and here more specifically, Google cannot respond with regard to devices, browsers, applications, or other products and services that it does not create, own, or control. We respond to this Demand for Information to the extent possible based on information regarding Google Account-level settings, Android on Pixel devices, and as a general matter, with regard to Google products and services.

Pixel Devices. On the Pixel (and many third-party Android devices), users may grant their express consent for individual third-party apps to access the Android device location permission. The settings that allow a user to control this access are explained further below in response to Demand for Information No. 7.

Google Products and Services. Certain Google products and services may have an option or a setting that allow a user to choose to share user location with a third party. Given the number of Google products and services, it is not possible for Google to respond to this overbroad and burdensome request with regard to each product and service.

Location History, Web & App Activity, Usage & Diagnostics. Information on a specific user's location that Google collects via Google Account and device settings for Location History, Usage & Diagnostics, and Web & App Activity is not shared with third parties. However, aggregated and anonymized information that cannot be used to identify the location of a particular user is used by Google and third parties to develop and improve products, for system optimization, advertising, and other purposes.

Google Location Sharing. Google Location Sharing is the only Google Account setting that allows a user to choose to share his or her location with third parties. Please refer to our response to Demand for Information No. 7 for how users control that setting and the sharing of location information with third parties.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
In Google's February 28, 2019 letter to the AGO and in its first response to the First CID, Google objected to requests to the extent that they were overly broad and unduly burdensome in defining a

Relevant Time Period of more than 10 years—January 1, 2007 - present—across such a broad range of products and services. Google explained that in the absence of appropriate limitations, the scope was not manageable and made it difficult for Google to provide useful information in a timely and efficient manner. Subject to and without waiving those objections, Google provided detailed and substantive narrative responses and produced documents.

Google's April 17, 2019 response explained the specific controls available for users to manage the sharing of location information to third parties for Pixel Devices, certain Google products and services, Location History, Web & App Activity, and Google Location Sharing. In its June 20, 2019 supplemental response, Google asserted that "it ha[d] fully responded" and said "[i]f there are follow-up questions regarding this response" to "please let us know."

Additionally, Google made three witnesses available for examinations under oath, who were prepared to speak about the disclosure to third parties, if any, of user location information collected in connection with Android and Google Accounts. Further, as we mutually agreed, Google is making a fourth witness available for examination under oath later this month to speak about the disclosure to third parties, if any, of user location information collected in connection with Google-authored apps and Google search through a web browser.

Your January 17 letter asked for additional information about the types of situations in which data is shared with third parties, what precisely is shared, and the frequency of this sharing. Again, Google reasserts its objections to the breadth of this question, but provides additional examples and information below. Google would also like to reiterate that it has produced thousands of pages of documents that contain additional responsive information.

- Store Sales Visits

This is a feature that Google offers to a select group of approved advertising customers that uses aggregated and anonymized data from users that have opted into Location History to tell advertisers how their online ad clicks and viewable impressions influence physical store visits. Only certain advertising customers are approved. The feature is not available to advertisers with sensitive location categories related to healthcare, religion, adult content, and children. In addition, advertisers must meet certain criteria such as having sufficient store visits data on the backend to attribute to ad click or viewable impressions traffic and pass Google's user privacy thresholds.

The data that Google provides to advertisers is an aggregated statistic. It will show, for example, how an increase of x% in ad spend, can result in y% increase in store visits and z% increase in online conversions. Store visit data is based on anonymous, aggregated statistics, using differential privacy

techniques from which users cannot be reidentified. Google creates modeled numbers by using current and past data on the number of people who click or view an advertiser's ads and later visit their store. Store visit data cannot be tied to individual ad clicks, viewable impressions, or people. The data is available to advertisers to access in their Google Ads account at any time.

- Emergency Location Services (ELS) / [redacted]

Android Emergency Location Services (ELS) helps mobile network operators, emergency infrastructure providers, and governments provide more accurate location information to first responders during an emergency. ELS uses the location technologies on an Android phone, including cell, GPS and WiFi signals, and device sensors, to estimate an accurate emergency location. The location is often [redacted] and is calculated by the [redacted] ELS is solely for the use of emergency service providers, and location is sent from the user's device to emergency services only when the user explicitly places an emergency call, either directly or through their mobile network.

- **Google Person Finder**

On several occasions of catastrophe—such as during large earthquakes, tsunamis, or acts of terrorism—Google has made its Person Finder application available to users. This application is a message board-like service that, with a user's consent, allows them to share their current location and other pertinent information with a wide audience to facilitate their rescue by emergency services personnel or reunite them with family members.

Demands for Information Regarding User Privacy Controls

DEMAND FOR INFORMATION NO. 7
Explain whether and how a user can prevent Google or any third party from collecting his or her location data in connection with Android, Google-authored apps, Google search through a web browser, and Google Accounts.

INITIAL RESPONSE (April 17, 2019): Users have a number of options to control how their location information is collected and shared. For example, users can enable or disable device location controls, as well as deny apps access to location on an app-by-app level. Specifically, users can adjust the following device or Google Account settings:

Devices

- **Device's Location Setting**

On the Pixel (and many Android devices), a device-level setting controls device-based location. When the device's location setting is on, apps with the user's permission can access the device's location. Users can change the setting at any time in the "Security & location" panel of their Pixel. If a user disables this setting for their device, then no apps can access the device's location. Note that apps or websites connecting to the Internet may continue to use other signals like IP address, or other information the user provides, to infer information about the user's location. Google, for example, may use IP-based location to prevent abuse or to ensure users get search results that are relevant to their location (for example, people searching for "football" in England likely want different results than people searching for "football" in the U.S.).

- **Google Location Accuracy (formerly known as Google Location Services) ("GLA")**

GLA is a network-based location service that collects data to improve location accuracy and provide certain location information to the apps and services with the requisite permissions. Users can change the setting at any time from their Pixel device's "Security & location" panel. The information Google collects from GLA is linked to a temporary and rotating device identifier that is not used by or shared with other services. It is not connected with any identifier that would associate that data with a specific user.

- **Usage & Diagnostics**

The optional Usage & Diagnostics setting helps Google improve Android OS based on information about how devices are used and work. When this setting is enabled, Google collects IP addresses. When the Usage & Diagnostic setting is disabled, Google may still collect user location information via other relevant settings.

Google Account

- **Location History**

This is a distinct product Google provides to Google Account holders that saves a private map (that is not accessible to or shared with third parties) of where the user goes with his or her signed-in devices, even when the user is not using a Google service. Location History is disabled by default and users must opt in to enable it. Opting in to Location History allows Google to build a user's Timeline (which users can review and delete at any time at https://maps.google.com/timeline) of the places the user's devices have been and to provide more personalized features across Google products and services, such as traffic predictions for their daily commute.

- **Web & App Activity**

This is a Google Account setting that stores a user's Google activity data to My Activity (https://myactivity.google.com) in their Google Account. The user location information that is saved

as a result of Web & App Activity (which users can review and delete in My Activity at any time) is collected and stored in a user's Google Account when the user is engaging with a Google product and has Web & App Activity enabled. For example, when a user uses Google Search or Google Maps to search for "restaurant," Google collects the search term as well as information about that activity, including IP address and location information, so that the search results returned to the user will show nearby restaurant options.

- **Google Location Sharing**

Google Location Sharing allows Account holders to share their real-time location with others. Account holders choose whom they want to share their location with and for how long. For example, a user may share their estimated time of arrival with a friend once they are navigating on a journey to see them. A user may also create a share that will expire after a defined period of time, such as with friends during a vacation. Finally, a user may create an ongoing share (for example, with a family member) and decide to stop the share at a later date.

Google provides users centralized dashboards to control their Account-level and device-level location, privacy, and security settings.

Additionally, and as we explain above in response to Demand for Information No. 4, users can manage device location settings in the "Security and location" settings and their Google Account settings at https://myaccount.google.com/activitycontrols. Users can remove Location History entries from their Timeline at any time and Web & App Activity entries from their My Activity page at any time.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 8
Explain whether and how a user can entirely prevent Google or any third party from collecting his or her location data.

INITIAL RESPONSE (April 17, 2019): Google cannot respond with regard to users' interactions with third parties, nor can it respond with regard to mobile devices that have settings that are neither designed nor controlled by Google. Google focuses its response on Google Account settings that control the collection and use of location information for Location History, Web & App Activity, and Google Location Sharing, as well as certain Pixel device level settings.

The CID defines "User location data" as "any data from which a user's location can be determined, including but not limited to location information collected through device sensors, GPS, Wi-Fi,

Bluetooth, cell towers, and IP addresses." As Google explains in its Privacy Policy, mobile device and Google Account settings enable users to manage location information collection. As a general matter, IP addresses are required for devices to be able to connect to one another through the Internet and are necessary for online services to function. As a result, in order to use and interact with products and services from mobile and other devices, IP address information is transmitted when device or Account settings are disabled.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
As Google has previously explained, in order to use and interact with products and services from mobile and other devices, IP address information is transmitted when device or Account settings are disabled. Among other things, this information helps Google approximate the location of its users to comply with certain legal requirements, such as restrictions on the supply of gambling services or advertising services, which differ by jurisdiction. Google may also collect, store, and use location information to help detect fraud or other suspicious activity on a user's account. In addition, IP address information may enable users to determine when their Google Accounts have been compromised by unusual activity.

DEMAND FOR INFORMATION NO. 9
Explain whether and how, during the set up process for an Android device, the user can turn off any settings, functions, or permissions relating to the collection of user location data, and identify any such settings, functions, or permissions that the user cannot turn off at that point.

INITIAL RESPONSE (April 17, 2019): As described in our General Objections, it is not possible for Google to provide responses regarding the numerous manufacturers and variations and versions of Android devices they design, develop, or market. These devices may have different user interfaces and settings. Consistent with our objections, Google's response to this Demand for Information is thus limited to Pixel devices.

When a user sets up a Pixel-running Android Pie (version 9.0 and up), they are prompted to manage the device location setting. The user's choice for this setting will also apply to the Google Location Accuracy ("GLA") setting described in response to Demand for Information No. 8 above. On Pixel devices running older versions of Android, users were presented with an option to manage the GLA setting during set up and would exit the set up with the device location toggle setting enabled. Users can manage these settings any time after device set up.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 10
Explain whether and how, after completing the set up process for an Android device, the user can turn off any settings, functions, or permissions relating to the collection of user location data, and identify any such settings, functions, or permissions that the user cannot turn off after the set up process.

INITIAL RESPONSE (April 17, 2019): As described in our General Objections, it is not possible for Google to provide responses regarding the numerous manufacturers and variations and versions of Android devices they design, develop, or market. These devices may have different user interfaces and settings. Consistent with our objections, Google's response to this Demand for Information is thus limited to Pixel devices.

At any time after setting up a Pixel device, a user can disable any or all of the device settings, functions, or permissions described above in response to Demand for Information No. 7.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 11
Explain whether and how Google collects, stores, uses, deletes, and discloses user location data when the user turns off the Location History setting of his or her Google Account but keeps the Web & App Activity setting turned on.

INITIAL RESPONSE (April 17, 2019): The Web & App Activity Google Account setting is described above in Demand for Information No. 7. It is a distinct and separate Google Account setting from Location History. Users can access and manage the Web & App Activity Google Account setting at any time from their Google Account.

As we explain in our Privacy Policy and above in response to Demands for Information Nos. 1-4 the user location information that Google collects and stores depends on a number of factors, including the product or service being used and an individual user's settings. When a user pauses Location History, Google presents specific disclosures to remind the user that Google may still use location information that we received from their use of other Google products or services.

If a user has Web & App Activity enabled, when they use a Google service, like Google Maps or Search, Google may process information about that activity including location information. Google discloses how it handles user data in the Google Privacy Policy (available at https://policies.google.com/privacy) and Location Data page (available at https://policies.google.com/technologies/location-data), within the Web & App Activity setting itself, and in various publicly-available help center pages. When Web & App Activity is enabled, certain user location information is stored with the user's Google Account alongside the activity and can be viewed, managed, and deleted in My Activity (available at https://myaccount.google.com/activitycontrols).

As a general matter, as described above, IP addresses are required for devices to be able to connect to one another through the Internet and are necessary for online services to function. As a result, in order to use and interact with products and services from mobile and other devices, IP address information is transmitted, even when location settings are disabled.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 12
Describe the user location data that Google collects (including through the Android operating system or through Google-authored apps or Google websites running or accessed through an Android device or iOS device) when the user turns off both the Location History and the Web & App Activity settings of his or her Google Account, including location data collected through IP addresses, GPS, Wi-Fi scanning, Bluetooth scanning, cell tower information, barometer, or any other sensors.

INITIAL RESPONSE (April 17, 2019): As we explain in our Privacy Policy and above in response to Demands for Information Nos. 1-4, the user location information that Google collects and stores depends on a number of factors, including the product or service being used and an individual user's settings. As we explain above in response to Demand for Information No. 7, the Location History and Web & App Activity settings are distinct Google Account settings that a user can choose to enable or disable at any time. These Google Account settings do not affect or control device settings, which vary based on the specific device and which Google does not create or control.

Android or iOS mobile devices have settings that enable users to control the collection of device-based location information. IP addresses are required for devices to be able to connect to the Internet and are necessary for online services to function. As a result, in order to use and interact with products and services from mobile and other devices, IP address information is transmitted, even when location settings are disabled.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 13
Explain whether and how Google collects, stores, uses, deletes, and discloses user location data when the user turns off the Location setting of an Android device, and describe the user location data so collected.

INITIAL RESPONSE (April 17, 2019): Please refer to our responses to Demands for Information Nos. 10-12.

SUPPLEMENTAL RESPONSE (June 20, 2019): Please also refer to our response to Demand for Information No. 7. Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 14
Explain whether and how Google collects, stores, uses, deletes, and discloses the location data of any user of a device made by an entity other than Google, but on which the user has installed a Google-authored app or through which the user accesses a Google Account, when the user has otherwise disabled location tracking on the device.

INITIAL RESPONSE (April 17, 2019): As described in our General Objections, Google cannot respond with regard to the conduct of third parties, nor can it respond with regard to Android or other devices that have settings that are neither designed or controlled by Google.

With regard to Google Account settings, and Google's collection and use of location information when a user has disabled locating settings, please refer to our responses to Demands for Information Nos. 10-12.

Given the number of Google products and services, it is not possible for Google to respond to this overbroad and burdensome request with regard to each product and service that a user may install on a mobile device.

As a general matter, as described above, IP addresses are required for devices to be able to connect to one another through the Internet and are necessary for online services to function. As a result, in order to use and interact with products and services from mobile and other devices, IP address information is transmitted, even when location settings are disabled.

SUPPLEMENTAL RESPONSE (June 20, 2019): Please also refer to our response to Demand for Information No. 7. Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 15
Explain the means by which third-party apps accessible through Android collect user location data, including when (a) the user turns off the Location setting of the device, (b) the user turns off the Location History setting of his or her Google Account but leaves the Web & App Activity setting turned on, and (c) the user turns off both the Location History and the Web & App Activity settings, and describe the user location data collected in all such cases.

INITIAL RESPONSE (April 17, 2019): As we explain above in response to Demands for Information Nos. 7 and 12, Location History and Web & App Activity are distinct Google Account features that a user can choose to enable or disable at any time. These Google Account settings do not affect or control mobile device settings, which vary based on the specific device. As we explain above in response to Demand for Information No. 2, mobile devices have settings that enable users to control the collection of device-based location information. Also, as described in our General Objections, Google cannot respond with regard to the conduct of third parties, nor can it respond with regard to Android or other devices that have settings that are neither designed or controlled by Google.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 16
Explain how users can delete the user location data Google collects in connection with Android, Google-authored apps, Google search through a web browser, and Google Accounts.

INITIAL RESPONSE (April 17, 2019): We address deletion of location information in our responses to Demands for Information Nos. 2, 4, and 11 above.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 17
Explain whether and how user location data is collected through the Location History setting even when the user turns off that setting, and then stored once the user turns that setting back on.

INITIAL RESPONSE (April 17, 2019): As we explain above in response to Demand for Information No. 7, Location History is a distinct product that allows Google Account holders to save a private map of where the user goes with his or her signed-in devices. Opting in to Location History allows Google to build a private Timeline of the places the user's devices have been and to provide more personalized products and services, such as traffic predictions for their daily commute. Google stores Timeline information until an Account holder edits or deletes it. Account holders can disable Location History at any time, and they can edit or delete their Timeline at any time.

When Location History is paused, the product no longer saves the user's location information to the user's private Timeline (users can also opt out a particular device from collecting and reporting user location to Location History). However, pausing Location History—the distinct product—does not disable other settings that affect the collection of user location information (e.g., IP addresses).

When a user pauses Location History, Google presents specific disclosures to remind him or her that Google may still use location information that Google receives from his or her use of other products and services. For example, if a user has Web & App Activity enabled, when they use a Google product or service like Google Maps or Search, Google may process user location information including the device's IP address and other user location information.

Google discloses how it collects user data, including location information, in its Privacy Policy (available at https://policies.google.com/privacy), on the Location Data page (available at https://policies.google.com/technologies/location-data), and within the settings described above, in response to Demand for Information No. 7, and in help center pages.

SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Demand for Information, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

Demands for Information Regarding Tracking of Arizonans

DEMAND FOR INFORMATION NO. 18
Identify the number of users in Arizona whose location data you have collected in connection with Android, Google-authored apps, Google search through a web browser, and Google Accounts. Specify the number of Arizona users whose location data you collected even when (a) the user had turned off the Location setting of his or her Android device, (b) the user had turned off the Location History setting of his or her Google Account but left the Web & App Activity setting turned on, and (c) the user had turned off both the Location History and the Web & App Activity settings.

INITIAL RESPONSE (April 17, 2019): In the ordinary course of its business, Google does not determine, or maintain any document stating, the number of users in Arizona who have had Google Accounts during certain periods of time. Neither does Google, in the regular course of its business, determine or maintain any document stating, the number of users in Arizona who may have had Location History or Web & App Activity enabled or paused.

SUPPLEMENTAL RESPONSE (June 20, 2019): As previously stated, Google does not maintain such documents in the ordinary course of business. We are currently attempting to ascertain whether this information can be determined through other means. We will update you on our progress.

THIRD SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google has not identified information maintained in the ordinary course that states the number of users in the manner described in DFI 18. However, with regard to the specific scenarios described in (a)-(c) of DFI 18, as we have previously explained, the user location information that Google collects and stores depends on a number of factors, including the product or service being used and an individual user's settings. For instance, every device connected to the Internet is assigned an IP address and these numbers are usually assigned in geographic blocks. Thus, an IP address can often be used to identify the location from which a device is connecting to the Internet.

When a user pauses Location History, Google presents specific disclosures to remind the user that Google may still use location information that we received from their use of other Google products or services.

Google explains in its Privacy Policy (available at https://policies.google.com/privacy), and in additional disclosures on the page titled How Google Uses Location Information (available at https://policies.google.com/technologies/location-data and produced in documents Bates- stamped GOOG-GLAZ-00002725 - GOOG-GLAZ-00002727, GOOG-GLAZ-00002734 - GOOG-GLAZ-00002782, and GOOG-GLAZ-00002794 - GOOG-GLAZ-00002811), that Google collects IP addresses.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 19
Identify the number of times that you have refused to disclose the user location data, however collected, of any Arizonan when requested by any third party, including law enforcement.

INITIAL RESPONSE (April 17, 2019): Google objects to this Demand for Information as vague and ambiguous, overly broad, and irrelevant to any investigation under the Arizona Consumer Fraud Act. Subject to and without waiving its objections, Google refers the AGO to its semi-annual Transparency Report, which provides information about the requests for user data Google receives from government agencies, courts, and parties in civil litigation (https://transparencyreport.google.com/).

SUPPLEMENTAL RESPONSE (June 20, 2019): Google continues to object to this request, including for the reasons stated previously. Google does not maintain the data requested on a state-by-state basis. National data, among others, is in the Transparency Report discussed below.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 20
Identify all third-party advertising firms that you worked with to create TV, print, video, and digital ads run or viewed in Arizona relating to Android, Google-authored apps, Google search through a web browser, and Google Accounts. (Examples would include the T-Mobile G1 ads run in 2008, the "be together. not the same." ad campaign run during 2014-2016, and the Fred Rogers ad run in 2018.) For each such advertising firm, also provide the relevant dates, the names/titles of the advertising campaigns, and the types of ads created.

INITIAL RESPONSE (April 17, 2019): We object to this Demand for Information as unduly broad, overly burdensome, and irrelevant to the extent that it seeks information about advertisements that

do not relate to the collection, use, or disclosure of user location information, which appears to be the focus of the Attorney General's investigation.

SUPPLEMENTAL RESPONSE (June 20, 2019): Google continues to object to this request, including for the reasons stated previously.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google continues to object as stated above. This item has not been the subject of any discussion between Google and the AGO to date.

Demands for Information Relating to Responses to This Civil Investigation Demand

DEMAND FOR INFORMATION NO. 21
Identify all natural persons from whom documents were collected for possible production by respondent in response to this Civil Investigative Demand (i.e., "custodians") and the specific Bates range in the production applicable to each custodian.

INITIAL RESPONSE (April 17, 2019): Google did not collect any documents from individual custodians in order to prepare its response to this CID.

SUPPLEMENTAL RESPONSE (June 20, 2019): Documents were collected from [redacted] and [redacted] and are labeled GOOG-GLAZ-00001205 to GOOG-GLAZ-1479.

FINAL RESPONSE:
Google has collected documents from these custodians:

[redacted]

DEMAND FOR INFORMATION NO. 22
To the best of your knowledge and belief, are you producing or otherwise making available for examination with your response to this Civil Investigative Demand all non-privileged documents responsive to numbers 1–21 of the Requests to Produce Documents, below, that are in your possession, custody, or control?

INITIAL RESPONSE (April 17, 2019): Subject to the responses and the objections set forth here and in Google's February 28, 2019 letter, Google is producing non-privileged, responsive information.

SUPPLEMENTAL RESPONSE (June 20, 2019): As stated above, Google's effort to comply with the broad requests contained in the AGO's RFPs is ongoing and includes continued production of responsive, non-privileged materials. Google will continue to update the AGO on the status of Google's efforts, including when its anticipated production is complete.

FINAL RESPONSE:
As of the date of this response, Google asserts that it has completed its document production of responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating certain feedback from the AGO.

DEMAND FOR INFORMATION NO. 23
To the extent that your answer to demand 22 is not an unequivocal "yes," are the reasons why all non-privileged, responsive documents in your possession, custody, or control are not being collected and produced set forth in the response to each request in accordance with the instructions?

INITIAL RESPONSE (April 17, 2019): Google has asserted responses and objections here and in our February 28, 2019 letter.

SUPPLEMENTAL RESPONSE (June 20, 2019): Google has provided these Supplemental Responses as part of its continuing effort to respond to the AGO's numerous demands for investigative discovery. Google's efforts are ongoing and a complete catalogue of those efforts and their results cannot be provided at this time. Google has described above the status of its efforts, the currently-known limitations thereon, and other information related to their status. Google will continue to update the AGO on the status of its efforts, including when its anticipated production is complete.

FINAL RESPONSE:
As of the date of this response, Google asserts that it has completed its document production of responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating certain feedback from the AGO.

II. REQUESTS TO PRODUCE DOCUMENTS

REQUEST FOR PRODUCTION NO. 1
Produce all DOCUMENTS referenced, reviewed, or relied on in providing your responses to the above demands for information in this Civil Investigative Demand. In your response below, provide the specific bates range(s) for these documents and identify the demand(s) for information to which each document applies.

INITIAL RESPONSE (April 17, 2019): Google is producing with its response, as Bates-stamped GOOG-GLAZ-00000001 to GOOG-GLAZ-00000057 and GOOG-GLAZ-00000871 to GOOG-GLAZ-00000875, copies of the following records:

https://policies.google.com/privacy (DFIs Nos. 1, 11, 17)
https://policies.google.com/technologies/retention (DFIs Nos. 4)
https://policies.google.com/technologies/location-data (DFIs Nos. 5, 11, 17)
https://support.google.com/transparencyreport/answer/7381738 (DFIs Nos. 19)
https://transparencyreport.google.com/user-data/overview (DFIs Nos. 19)

SUPPLEMENTAL RESPONSE (May 30, 2019): Google has produced responsive documents and cited them in its initial response.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Based on our understanding of this Request for Production, Google asserts that it has fully responded to it. If there are follow-up questions regarding this response, please let us know.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO 2
Produce organizational charts or other similar documents sufficient to show the names of the relevant present and former Google employees with responsibilities for each of the following areas as they relate to Android, Google-authored apps, Google search through a web browser, and Google Accounts used by consumers in Arizona. Account for the full relevant time period.

a. The user set up process for Android mobile devices after a user turns it on for the first time.
b. The collection, storage, use, deletion, and disclosure of user location data relating to Google-authored apps running on Android and iOS mobile devices.
c. The collection, storage, use, deletion, and disclosure of user location data relating to Google searches run on Android and iOS mobile devices.

d. The Settings app/panel in Android and any settings that relate to the collection, storage, use, deletion, or disclosure of any user location data.
e. Google Accounts and any settings, functions, and permissions on Google Accounts that relate to the collection, storage, use, deletion, or disclosure of any user location data.
f. Advertising to consumers relating to Android, Google-authored apps, Google search through a web browser, and Google Accounts.
g. Communications with users (including tutorials, help pages and videos, "how to" pages and videos, and blog posts) relating to settings on Android, Google-authored apps, Google search through a web browser, or Google Accounts and the collection, storage, use, deletion, or disclosure of any user location data collected through Android mobile devices, Google-authored apps, Google search through a web browser, and Google Accounts.
h. User privacy for Android, Google-authored apps, Google search through a web browser, and Google Accounts relating to the collection, storage, use, deletion, or disclosure of any user location data.
i. Google's marketing and sales to advertisers of any and all types of location-aware advertising products and services (including targeting ads to specific locations or interests, local campaigns, tracking the effectiveness of online ads at driving foot traffic, and building user profiles for ads based in part on the user's location data).
j. Google's communications to third-party developers relating to the collection, storage, use, deletion, and disclosure of user location data collected by such third-party apps running on Android.

INITIAL RESPONSE (April 17, 2019): Google objects to this request as overly broad and unduly burdensome in seeking organizational charts for detailed functions that would not constitute one unit or division of employees at Google. Google does not maintain, in the ordinary course of business, organizational charts of this type, and would be forced to create extensive work product that would not remain current once generated. Additionally, it is not clear how all of these documents being requested for all the topics listed above are relevant to the location-related requests.

SUPPLEMENTAL RESPONSE (May 30, 2019): In the absence of more detailed guidance regarding the AGO's investigation, Google does not understand the relevance of this Request to the AGO's location-focused investigation and therefore reiterates its objection on this ground. In addition, Google reiterates that it does not maintain organizational charts in the ordinary course of business. In order to provide responsive information to the AGO's investigation as we understand it, Google notes that the person most knowledgeable about Location History is [redacted] and the person most knowledgeable about Web & App Activity is [redacted]

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): As discussed during our last telephone call, to answer this request Google is instead providing the following information:

Google has previously responded that the person most knowledgeable about Location History is [redacted]), and the person most knowledgeable about Web & App Activity is [redacted]). Google is in the process of collecting and producing responsive, non-privileged records for which these two employees were custodians.

Mr [redacted] reports to [redacted]. Mr. [redacted] reports to [redacted] And Mr. [redacted] reports to senior management. Google reiterates that Mr. [redacted] is the person most knowledgeable about Location History.

Mr [redacted] reports to [redacted] Mr. [redacted] reports to [redacted] And Mr. [redacted] reports to senior management. Google reiterates that Mr [redacted] is the person most knowledgeable about Web & App Activity.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO 3
Produce a representative example of the complete user set up process in English (including all screens seen by the user and showing all pictures, icons, text, and pop-ups visible to the user, and all linked documents such Google's terms of use and privacy policy) for each version of the set up process for Android mobile devices used in Arizona during the relevant time period.

INITIAL RESPONSE (April 17, 2019): Google is producing documents Bates-stamped GOOG-GLAZ-00000058 to GOOG-GLAZ-00000128. Google's response to this RFP is limited to Pixel devices. The first Google Pixel device was released in October 2016. Google's response to this RFP is limited to January 1, 2017 - January 30, 2019.

Please see the documents Bates-stamped GOOG-GLAZ-00000491 to GOOG-GLAZ-00000781, for the Google Terms of Service and Privacy Policy in effect from January 1, 2017 - January 30, 2019.
SUPPLEMENTAL RESPONSE (May 30, 2019): Google has produced a responsive representative example and cited it in its initial response.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google has conducted a diligent search for and previously produced all responsive documents regarding the set up of Pixel devices.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 4
Produce documents (including screen shots or images) sufficient to show all portions of the Settings app/panel on Android relevant to turning on or off particular settings, functions, or permissions relating to Location, Web & App Activity, and Location History for all versions of Android used in Arizona during the relevant time period, as well as all notifications or other explanations provided to users when turning on or off any of the foregoing.

INITIAL RESPONSE (April 17, 2019): Google is producing documents Bates-stamped GOOG-GLAZ-00000129 to GOOG-GLAZ-00000149. Google's response to this RFP is limited to Pixel devices. The first Google Pixel device was released in October 2016. Google's response to this RFP is limited to January 1, 2017 - January 30, 2019.

SUPPLEMENTAL RESPONSE (May 30, 2019): Google has produced responsive documents and cited them in its initial response.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google has conducted a diligent search for and previously produced all responsive documents regarding the relevant settings of Pixel devices.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 5: Produce documents (including screen shots or images) sufficient to show all portions of the Google Accounts website relevant to users in Arizona during the relevant time period turning on or off particular settings, functions, or permissions relating to the collection, storage, use, deletion, or disclosure of any user location data, as well as all notifications or other explanations provided to users when turning on or off any of the foregoing.

INITIAL RESPONSE (April 17, 2019): Google is producing documents Bates-stamped GOOG-GLAZ-00000150 to GOOG-GLAZ-00000170. Google's response to this RFP is limited to January 1, 2017 - January 30, 2019.

SUPPLEMENTAL RESPONSE (May 30, 2019): Google has produced responsive documents and cited them in its initial response.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google is producing responsive documents Bates-stamped GOOG-GLAZ-00001114 to GOOG-GLAZ-00001141.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 6
Produce all support pages relating to Location, Location Services, Web & App Activity, My Activity, and Location History for Android mobile devices or Google Accounts used in Arizona during the relevant time period.

INITIAL RESPONSE (April 17, 2019): Google is producing documents Bates-stamped GOOG-GLAZ-00000171 to GOOG-GLAZ-00000427. As described in our Responses and Objections to the CID's Instructions, "Location" and "Location Services" can potentially refer to a broad range of settings and features that may have no connection to Google's products or services. For example, devices other than the Pixel may have device settings referred to as Location or Location Services. Google's response to this RFP is thus limited to statements made about the Pixel device location toggle and the Pixel setting Google Location Accuracy, as well as the requested Google Account features that control the collection of location information (i.e., Web & App Activity and Location History) between January 1, 2017 - January 30, 2019.

SUPPLEMENTAL RESPONSE (May 30, 2019): Google has produced responsive documents and cited them in its initial response. Google supplements its response with new responsive Help Center materials currently available online, Bates-stamped GOOG-GLAZ-00000876 to GOOG-GLAZ-00000949. Google anticipates producing by June 12, 2019 further responsive Help Center materials showing how they appeared online between January 30, 2019, and before today.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Earlier this week, Google produced documents Bates-stamped GOOG-GLAZ-00001059 to GOOG-GLAZ-00001113. These documents reflect additional prior versions of Google's Help Center pages.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 7
Produce the English versions of all contracts and policies with users in Arizona (including privacy policies and terms of service) relating to Android, Google-authored apps, Google search through a web browser, and Google Accounts for the relevant time period.

INITIAL RESPONSE (April 17, 2019): Google is producing documents Bates-stamped GOOG-GLAZ-00000428 to GOOG-GLAZ-00000781, the Google Terms of Service and Privacy Policy in effect from January 1, 2017 - January 30, 2019.

SUPPLEMENTAL RESPONSE (May 30, 2019): Google has produced responsive documents and cited them in its initial response.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google's prior productions included its Terms of Service and Privacy Policy in effect from January 1, 2017 - January 30, 2019. Google objects to further production on the grounds previously stated.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 8

Produce all contracts and policies with third-party Android app developers, and all Google advertisements, presentations, sales communications, videos, tutorials, webpages, and blog posts addressed to third-party app developers, relating to user location data.
INITIAL RESPONSE (April 17, 2019): Google is producing the following documents Bates-stamped GOOG-GLAZ-00000782 to GOOG-GLAZ-00000862:

Google APIs Terms of Service
Google API Services: User Data Policy
Google Play Developer Distribution Agreement
Google Play Developer Policy Center

SUPPLEMENTAL RESPONSE (May 30, 2019): Google has produced responsive documents and cited them in its initial response.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google's prior productions included its consumer-facing contracts and policies. Google objects to further production on the grounds previously stated.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 9
Produce a representative example of each television advertisement run in a geographic area including any part of Arizona by Google or a third-party partner of Google (such as a hardware manufacturer, telephone carrier, or electronics retailer) during the relevant time period relating to Android, Google-authored apps, Google search through a web browser, and Google Accounts.

INITIAL RESPONSE (April 17, 2019): Google objects to this Request for Production to the extent that it seeks information that is seemingly irrelevant to the Attorney General's investigation and/or outside of the scope of the Attorney General's investigatory authority. Google also does not maintain this information in the ordinary course of business as Google does not categorize the information requested by U.S. state.

Given the broad scope and timeframe for the request, it would help Google to respond if we understood how (if at all) these requests relate to the location-focused requests. The request on its face reflects an entirely separate topic.

SUPPLEMENTAL RESPONSE (May 30, 2019): In the absence of more detailed guidance regarding the AGO's investigation, Google does not understand the relevance of this Request to the AGO's location-focused investigation and therefore reiterates its objection on this ground. Subject to and without waiving Google's objections to this Request, since our meet-and-confer call on May 23, we have worked to identify television advertisements that are relevant to the AGO's investigation, as we understand it, that ran in a geographic area including any part of Arizona between January 1, 2017 and the present, and that are in Google's possession, custody, and control. As of today, we have not located television advertisements for Location History or Web & App Activity. If we locate any such responsive materials, we will promptly produce representative examples.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial relevancy objection and reasserts the other objections made. Google remains in the process of searching and reviewing for responsive documents. We will update you on our progress.

THIRD SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google previously conducted a search of information regarding the Geo product area, which includes Google Maps and other geo products, to find a representative sample of online advertisements that Google ran for the Location History, Web & App Activity, and Google Maps products. Google previously produced these advertisements to the AGO on June 20, 2019. Google has not located any responsive television advertisements.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 10
Produce a representative example of each print advertisement (e.g., newspaper ads, magazine ads) run in a geographic area including any part of Arizona by or on behalf of Google during the relevant time period relating to Android, Google-authored apps, Google search through a web browser, and Google Accounts.

INITIAL RESPONSE (April 17, 2019): Google objects to this Request for Production to the extent that it seeks information that is seemingly irrelevant to the Attorney General's investigation and/or

outside of the scope of the Attorney General's investigatory authority. Google also does not maintain this information in the ordinary course of business as Google does not categorize the information requested by U.S. state.

Given the broad scope and timeframe for the request, it would help Google to respond if we understood how (if at all) these requests relate to the location-focused requests. The request on its face reflects an entirely separate topic.

SUPPLEMENTAL RESPONSE (May 30, 2019): In the absence of more detailed guidance regarding the AGO's investigation, Google does not understand the relevance of this Request to the AGO's location-focused investigation and therefore reiterates its objection on this ground. Subject to and without waiving Google's objections to this Request, since our meet-and-confer call on May 23, we have worked to identify print advertisements that are relevant to the AGO's investigation, as we understand it, that ran in a geographic area including any part of Arizona between January 1, 2017 and the present and that are in Google's possession, custody, and control. As of today, we have not located print advertisements for Location History or Web & App Activity. If we locate any such responsive materials, we will promptly produce representative examples.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial relevancy objection and reasserts the other objections made. Google remains in the process of searching and reviewing for responsive documents. We will update you on our progress.

THIRD SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google previously conducted a search of information regarding the Geo product area, which includes Google Maps and other geo products, to find a representative sample of online advertisements that Google ran for the Location History, Web & App Activity, and Google Maps products. Google previously produced advertisements to the AGO on June 20, 2019. Google did not locate any responsive traditional print media advertisements, but did produce ads that ran online.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 11
Produce a representative example of each online advertisement (e.g., digital ads, text ads, pop-up ads, video ads, online ads) run in a geographic area including any part of Arizona by

Google or a third-party partner of Google (such as a hardware manufacturer, telephone carrier, or electronics retailer) during the relevant time period relating to Android, Google-authored apps, Google search through a web browser, and Google Accounts.

INITIAL RESPONSE (April 17, 2019): Google objects to this Request for Production to the extent that it seeks information that is seemingly irrelevant to the Attorney General's investigation and/or outside of the scope of the Attorney General's investigatory authority. Google does not maintain this information in the ordinary course of business as Google does not categorize the information requested by U.S. state.

SUPPLEMENTAL RESPONSE (May 30, 2019): In the absence of more detailed guidance regarding the AGO's investigation, Google does not understand the relevance of this Request to the AGO's location-focused investigation and therefore reiterates its objection on this ground. Subject to and without waiving Google's objections to this Request, since our meet-and-confer call on May 23, we have worked to identify online advertisements that are relevant to the AGO's investigation, as we understand it, that ran in a geographic area including any part of Arizona between January 1, 2017 and the present and that are in Google's possession, custody, and control. As of today, we have not located online advertisements for Location History or Web & App Activity. If we locate any such responsive materials, we will promptly produce representative examples.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial relevancy objection and reasserts the other objections made. Google is producing responsive documents Bates-stamped GOOG-GLAZ-00001142 to GOOG-GLAZ-00001204. Google remains in the process of searching and reviewing for responsive documents. We will update you on our progress.

THIRD SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google previously conducted a search of information regarding the Geo product area, which includes Google Maps and other geo products, to find a representative sample of online advertisements that Google ran for the Location History, Web & App Activity, and Google Maps products. Google previously produced advertisements to the AGO on June 20, 2019. Google has not identified additional responsive records within its possession, custody, or control.

FINAL RESPONSE:
After conducting a diligent search to respond to Requests for Production 9–11, on June 20, 2019, Google produced advertisements related to Location History, Web & App Activity, and Google Maps. In your letter dated January 17, 2020, you asked Google to provide the dates that the advertisements in question were first shown to the public.

The content produced in documents Bates-stamped GOOG-GLAZ-00001142 - GOOG-GLAZ-00001198 appeared on the Apple App Store Landing page (at https://apps.apple.com/us/app/google-maps-transit-food/id585027354) and the Google Play Store

landing page (at https://play.google.com/store/apps/details?id=com.google.android.apps.maps&hl=en_US), and was captured for production in June 2019. The product images on those pages were first made available on the following dates:

- GOOG-GLAZ-00001142 - GOOG-GLAZ-00001143, GOOG-GLAZ-00001180 - GOOG-GLAZ-00001182: 07/30/2018
- GOOG-GLAZ-00001162: GOOG-GLAZ-00001163,
- GOOG-GLAZ-00001165: 08/26/2016
- GOOG-GLAZ-00001164: Google is unable to determine the exact date the image in this document was first made available to the public, but it believes it was around March 2016.
- GOOG-GLAZ-00001195: 07/20/2018

For the YouTube files, Google is able to provide the below information and is also producing additional metadata in GOOG-GLAZ-00200233 - GOOG-GLAZ-00200237:

- GOOG-GLAZ-00001202: https://www.youtube.com/watch?v=7ZrW-_nKSfs (published 12/10/2018)
- GOOG-GLAZ-00001203: https://www.youtube.com/watch?v=ogfYd705cRs&feature=youtu.be&t=1h17m34s (published 05/08/2018)
- GOOG-GLAZ-00001204: https://www.youtube.com/watch?v=Q_XPrk824Vs&t=65s (published 12/13/2018)

For the Twitter files, Google is able to provide the following additional information:

- GOOG-GLAZ-00001199: https://twitter.com/googlemaps/status/861661514549219330 (published 05/08/2017; collected June 2019)
- GOOG-GLAZ-00001200: https://twitter.com/googlemaps/status/959456310197739520 (published 02/02/2018; collected June 2019)
- GOOG-GLAZ-00001201: https://twitter.com/googlemaps/status/966776119625121792 (published 02/ 22/2018; collected June 2019)

REQUEST FOR PRODUCTION NO. 12

Produce all tutorials, "how to" videos, or product explanations created by Google or a third-party partner of Google (such as a hardware manufacturer, telephone carrier, or electronic retailer) relating to the collection, storage, use, deletion, or disclosure of user location data

obtained from Android, Google-authored apps, Google search through a web browser, and Google Accounts.

INITIAL RESPONSE (April 17, 2019): Google objects to this Request for Production to the extent it seeks information not in the possession, custody, or control of Google. Google is producing files Bates-stamped GOOG-GLAZ-00000863 to GOOG-GLAZ-00000870, which include a video in the Google Privacy Policy under *Your location information*? And "Types of Location Information," https://policies.google.com/technologies/location-data.

SUPPLEMENTAL RESPONSE (May 30, 2019): Google has produced responsive materials and cited them in its initial response. Google supplements its response with new responsive material currently available online, Bates-stamped GOOG-GLAZ-00000950. Subject to and without waiving Google's objections to this Request, Google has conducted a reasonable search to identify responsive documents and to date has not identified additional responsive records within Google's possession, custody, or control.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial relevancy objection and reasserts the other objections made. Google remains in the process of searching and reviewing for responsive documents. We will update you on our progress

THIRD SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google has not identified additional responsive records within its possession, custody, or control.

FINAL RESPONSE:
In your letter dated January 17, 2020, you express surprise about the volume of Google's production in response to this Request. You also point to publicly-available material that you searched for and that you allege is responsive. The Request specifically asks for content that relates to "the collection, storage, use, deletion, or disclosure of user location data." In the context of the AGO's consumer-protection investigation, Google reasonably understood this Request to be seeking tutorials for Google users (in other words, consumers). The material you cite in your letter, however, is not such a tutorial. It is a marketing document that describes certain ads features for Google's advertising customers. So, it is neither a tutorial, nor is it aimed at consumers.

Google reiterates that it has conducted a reasonable search for, and has produced, responsive material. Complying with the breadth of the AGO's Request, which (i) covers every single Google product and service, (ii) spans more than thirteen years, and (iii) defines "user location data" to include IP addresses, which are required for all devices to be able to connect to the internet, is impossible. Google has made a good-faith effort to provide the AGO with relevant, useful, and responsive information by conducting a reasonable search for tutorial-like material aimed at Google consumers, and focused

on Google Account settings, that users can use to control the collection, storage, use, deletion, or disclosure of their location information.

REQUEST FOR PRODUCTION NO. 13
Produce all communications and other documents relating to the Associated Press article of August 13, 2018 entitled "Google tracks your movements, like it or not," including all communications and other documents relating to the changes you made after that article's publication to your representations about the collection, storage, use, or disclosure of user location data and about users' ability to prevent you and third parties from doing any of those things.

INITIAL RESPONSE (April 17, 2019): Google objects to the "all communications and other documents" scope of this Request for Production, as it is overly broad and unduly burdensome. To the extent this Request for Production seeks attorney-client privileged communications, Google also objects to producing such documents as protected by the privilege. Google is willing to meet and confer about an appropriate scope of information.

SUPPLEMENTAL RESPONSE (May 30, 2019): Subject to and without waiving Google's objections to this Request, Google is conducting a keyword search of the email records of relevant custodians to identify any non-privileged responsive documents. The search and review process is underway. Google currently anticipates that the process will be complete and any non-privileged responsive documents will be produced on or before June 12, 2019.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google is producing documents Bates-stamped GOOG-GLAZ-00001205 to GOOG-GLAZ-00001479. Google remains in the process of searching and reviewing for responsive documents. We will update you on our progress.

FINAL RESPONSE:
Based on our understanding of this Request for Production, Google has no additional information to provide related to it.

REQUEST FOR PRODUCTION NO. 14
Produce all communications and other documents relating to the New York Times article of December 10, 2018 entitled "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," including all communications and other documents relating to the changes you made after that article's publication to your representations about the collection, storage, use, or disclosure of user location data and about users' ability to prevent you and third parties from doing any of those things.

INITIAL RESPONSE (April 17, 2019): Google objects to the "all communications and other documents" scope of this Request for Production, as it is overly broad and unduly burdensome. To

the extent this Request for Production seeks attorney-client privileged communications, Google also objects to producing such documents as protected by the privilege. Google is willing to meet and confer about an appropriate scope of information.

SUPPLEMENTAL RESPONSE (May 30, 2019): Google continues to object to this request for the reasons stated below and as not relevant to the AGO's investigation of Google's policies, practices, and representations because the article referenced does not relate to or reference collection of location information when the Google Account settings Web & App Activity or Location History are enabled or disabled. Google is willing to search for responsive information if the AGO provides appropriate guidance on what aspects of this article are relevant to its investigation.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Absent clarification from the AGO on the relevance of this Request, Google reiterates its objections below.

FINAL RESPONSE:
Based on our understanding of this Request for Production, Google has no additional information to provide related to it.

REQUEST FOR PRODUCTION NO. 15
Produce documents sufficient to show the amount of money Google spent on advertising in Arizona (or, if such data is not state-specific, in the United States) relating to the Android operating system, Android devices, Google-authored apps, Google search through a web browser, and Google Accounts for each year during the relevant time period.

INITIAL RESPONSE (April 17, 2019): Google objects to this Request for Production to the extent it seeks sensitive and competitive business information. Additionally, Google objects to this Request for Production as Google does not maintain records in the ordinary course of business that categorize the information requested by U.S. state. Relatedly, because this Request for Production seeks information and data not connected to the state of Arizona and thus not relevant to this investigation, Google objects to this request as falling outside the Attorney General's authority related to this investigation. Preparing such information also would be unduly burdensome and difficult. Finally, Google does not understand how (if at all) this request relates to the location-focused requests as, on its face, it reflects an entirely separate topic.

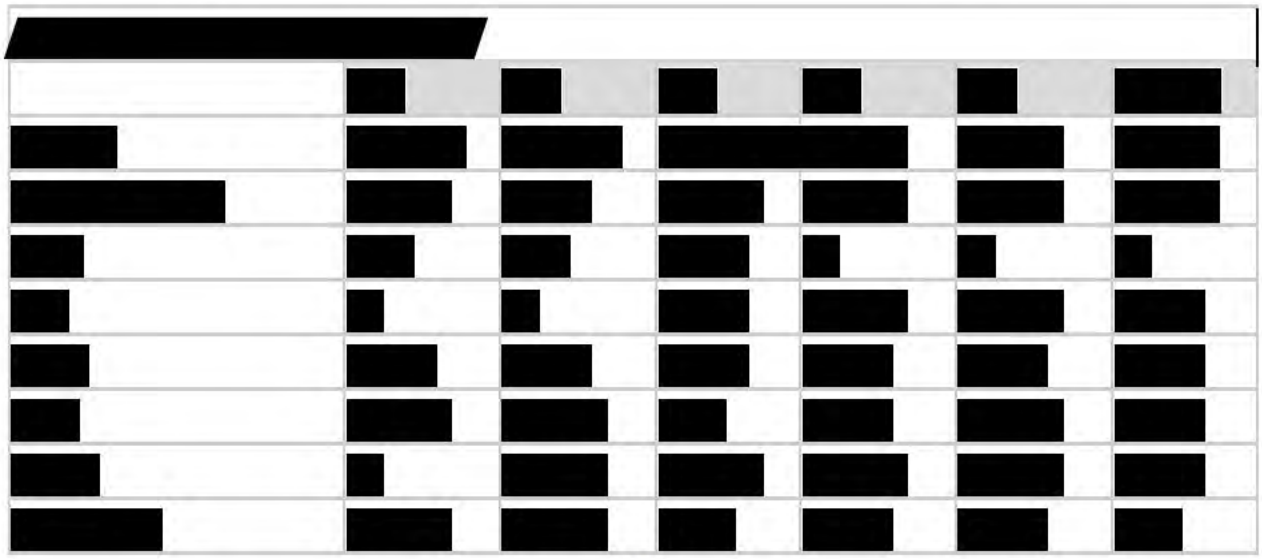
SUPPLEMENTAL RESPONSE (May 30, 2019): In the absence of more detailed guidance regarding the AGO's investigation, and because Google does not sell the location information of a specific Google user, Google does not understand the relevance of this Request to the AGO's location-focused investigation and therefore reiterates its objection on this ground. Subject to and without waiving Google's objections to this Request, since our meet-and-confer call on May 23, we have worked to identify television, print, and online advertisements that are relevant to the AGO's investigation, as we understand it, that ran in a geographic area including any part of Arizona between January 1, 2017 and the present and that are in Google's possession, custody, and control. As of today,

we have not located television, print, or online advertisements related to Location History or Web & App Activity. If we locate any such materials, we will promptly produce information relating to the advertising spend for those materials.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial relevancy objection and reasserts the other objections made. As previously stated, Google does not maintain such documents in the ordinary course of business. We are currently attempting to ascertain whether this information can be determined through other means. We will update you on our progress.

THIRD SUPPLEMENTAL RESPONSE (Sept. 4, 2019): Google does not maintain documentation collecting or summarizing the amounts that Google spent to advertise these Google products or services. Previous efforts to respond to this request focused on Location History or Web & App Activity alone, but Google now is attempting to determine the amount Google spends to advertise all these Google products and services. Because this request covers numerous Google products and services and because Google does not maintain a single document (or even several documents) collecting or summarizing these amounts, Google is unable to answer this request at this time. Google is working to attempt to determine this amount. Google will keep you updated on its progress and expected response date.

FOURTH SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google has not identified information kept in the ordinary course of business that specifically states the amount of money Google spent on advertising in Arizona relating to the Android operating system, Android devices, Google-authored apps, Google search through a web browser, and Google Accounts for each year during the relevant time period the number. In order to satisfy the Attorney General's request for information, Google has made an effort to estimate the marketing spend in the United States for the following Google Mobile Services and Android:



[redacted]						
[redacted]						
[redacted]						
[redacted]						

FINAL RESPONSE:
Your January 17, 2020 letter asked Google to supplement this response by including all Android devices for which Google has information in its possession, custody, or control. Google is able to additionally provide its marketing spend for Pixel mobile devices, but Google is not able to break down the data by device.

[redacted]					
[redacted]					

Your January 17, 2020 letter also asked Google to answer the following questions:

1. Which Google employees were involved in collecting or compiling this data? Please also identify their titles.

- [redacted]

2. Please explain where Google's figures are derived from. For example, from which documents, repositories or other systems was this data collected?

Google queried its Oracle Hyperion financial database.

3. Google stated that the figures it provided were estimates. Please explain how Google arrived at these estimates from the raw data.

For certain products, like [redacted], Google's marketing spend was combined with other communications products, so Google had to ask one of its financial data analysts to split the [redacted] marketing spend.

REQUEST FOR PRODUCTION NO. 16
Produce documents sufficient to show the number of users of the Android operating system in Arizona during the relevant time period.

INITIAL RESPONSE (April 17, 2019): In the ordinary course of its business, Google does not determine, or maintain any document stating, the number of users of the Android OS in Arizona. Further, Google objects to this Request for Production to the extent it seeks information regarding third-party Android devices, which is not under its possession, custody, or control.

SUPPLEMENTAL RESPONSE (May 30, 2019): Subject to and without waiving Google's objections to this Request, Google reiterates that it does not currently maintain an existing document stating the information sought by this Request. It is nonetheless in the process of trying to determine what, if any, information can be compiled to provide a substantive response to this Request and will further supplement this response as soon as possible.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial relevancy objection and reasserts the other objections made. As previously stated, Google does not maintain such documents in the ordinary course of business. We are currently attempting to ascertain whether this information can be determined through other means. We will update you on our progress.

THIRD SUPPLEMENTAL RESPONSE (Sept. 4, 2019): Google does not maintain an existing document stating the information sought by this Request. Google remains in the process of determining whether it can provide other information responsive to this request.

FOURTH SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google has not identified information kept in the ordinary course of business that specifically states the number of users of the Android operating system in Arizona during the relevant time period. Android is an open source software that can be used by anyone without a license. In order to satisfy the Attorney General's request for information, Google has made an effort to estimate the number of users of an Android operating system based on limited nationwide data available for device activations of Google-licensed Android mobile devices. Google estimates the number of Android devices in Arizona at:

- 2016 - [redacted]
- 2017 - [redacted]
- 2018 - [redacted]
- 2019 (January - July) - [redacted]

FINAL RESPONSE:
Your January 17, 2020 letter asked Google to answer the following questions:

1. Which Google employees were involved in collecting or compiling this data? Please also identify their titles.

Other than legal counsel, Google employees involved were:

- [redacted]
- [redacted]
- [redacted]

2. Please explain where Google's figures are derived from. For example, from which documents, repositories or other systems was this data collected?

In order to provide these estimates, Google had to query its Android Device Configuration Service database, which contains data related to Android device activation.

3. Google stated that the figures it provided were estimates. Please explain how Google arrived at these estimates from the raw data.

As we explained in our previous response dated December 31, 2019, Google has made an effort to estimate the number of users of an Android operating system based on limited nationwide data available for device activations of Google-licensed Android mobile devices. For the limited time period for which Google had this data, Google estimated Arizona numbers by counting activations with zipcodes inferred to be between 85001 and 86999.

REQUEST FOR PRODUCTION NO. 17
Produce documents sufficient to show the number of users of a Google Account, Google-authored app, or Google search through a web browser in Arizona during the relevant time period.

INITIAL RESPONSE (April 17, 2019): In the ordinary course of its business, Google does not determine, or maintain any document stating, the number of users of a Google Account, Google-authored app, or Google search through a web browser in Arizona. In addition, Google objects to this Request for Production to the extent it seeks information which is not under its possession, custody, or control.

SUPPLEMENTAL RESPONSE (May 30, 2019): Subject to and without waiving Google's objections to this Request, Google reiterates that it does not currently maintain an existing document stating the information sought by this Request. It is nonetheless in the process of trying to determine what, if any, information can be compiled to provide a substantive response to this Request and will further supplement this response as soon as possible.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial relevancy objection and reasserts the other objections made. As previously stated, Google does not maintain such documents in the ordinary course of business. We are currently attempting to ascertain whether this information can be determined through other means. We will update you on our progress.

THIRD SUPPLEMENTAL RESPONSE (Sept. 4, 2019): Google does not maintain an existing document stating the information sought by this Request. Google remains in the process of determining whether it can provide other information responsive to this request.

FOURTH SUPPLEMENTAL RESPONSE (Jan. 17, 2020): As we stated previously, Google does not maintain an existing document stating the information sought by this Request. Google undertook a reasonable effort to compile responsive data for this request. Based on available Google Account data, Google is providing monthly numbers (excluding prepay and terms customers) of purchases for the time period of Jan 2017 to November 2019, where the billing address of the form of payment used was associated with an Arizona zip code.[2]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[2] These numbers do not necessarily represent unique account holders across months and years.

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

FINAL RESPONSE:
Google responded to this request on January 17, 2020. Based on our understanding of this Request for Production, Google has no additional information to provide related to it.

REQUEST FOR PRODUCTION NO. 18
Produce documents sufficient to show the number of users for whom any location information was collected or stored as a result of the user's use of an Android mobile device, Google Account, Google-authored app, or Google search through a web browser, and for which the user was based in Arizona at any point during the relevant time period.

INITIAL RESPONSE (April 17, 2019): Google objects to this Request for Production as Google does not maintain this information in the ordinary course of business categorized by U.S. state. In addition, Google objects to this Request for Production to the extent it seeks information regarding third-party Android devices, which is not under its possession, custody, or control.

SUPPLEMENTAL RESPONSE (May 30, 2019): Subject to and without waiving Google's objections to this Request, Google reiterates that it does not currently maintain an existing document stating the information sought by this Request. It is nonetheless in the process of trying to determine what, if any, information can be compiled to provide a substantive response to this Request and will further supplement this response as soon as possible.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial relevancy objection and reasserts the other objections made. As previously stated, Google does not maintain such documents in the ordinary course of business. We are currently attempting to ascertain whether this information can be determined through other means. We will update you on our progress.

THIRD SUPPLEMENTAL RESPONSE (Sept. 4, 2019): As Google explains in its Privacy Policy (available at https://policies.google.com/privacy), in additional disclosures on the page titled How Google Uses Location Information (available at https://policies.google.com/technologies/ location-data and produced in documents Bates-stamped GOOG-GLAZ-00002725 - GOOG-GLAZ-00002727, GOOG-GLAZ-00002734 - GOOG-GLAZ-00002782, and GOOG-GLAZ-00002794 - GOOG-GLAZ-00002811), Google collects IP addresses. Every device connected to the Internet is assigned an IP address and these numbers are usually assigned in geographic blocks. Thus, an IP address can often be used to identify the location from which a device is connecting to the Internet.

FINAL RESPONSE:
As Google previously stated, Google collects IP addresses, which the AGO included in its definition of "User Location Data." See, e.g., First Civil Investigative Demand, pg. 6 ("'User location data' means any data from which a user's location can be determined, including but not limited to location information collected through device sensors, GPS, Wi-Fi, Bluetooth, cell towers, and IP addresses."). Google explains in its Privacy Policy (available at https://policies.google.com/privacy) and in additional disclosures on the page titled How Google Uses Location Information (available at https://policies.google.com/technologies/location-data and produced in documents Bates-stamped GOOG-GLAZ-00002725 - GOOG-GLAZ-00002727, GOOG-GLAZ-00002734 - GOOG-GLAZ-00002782, and GOOG-GLAZ-00002794 - GOOG-GLAZ-00002811), that Google collects IP addresses.

Google has previously produced a number of other responsive documents including but not limited to:

- GOOG-GLAZ-00080897 - GOOG-GLAZ-00080951: "Growth Opportunities for Location."

REQUEST FOR PRODUCTION NO. 19
Produce documents sufficient to show the revenue Google received from the use by consumers of Android mobile devices in Arizona, including revenue from advertisements displayed to users of Android devices in Arizona during the relevant time period.

INITIAL RESPONSE (April 17, 2019): Google objects to this Request for Production to the extent it seeks sensitive and competitive business information. Google also objects to this Request for Production as Google does not maintain this information in the ordinary course of business categorized by U.S. state. Preparing such information would be burdensome and difficult. In addition, Google objects to this Request as seeking information irrelevant to this investigation.

SUPPLEMENTAL RESPONSE (May 30, 2019): Google reasserts its initial relevancy objection, and reasserts the other objections made below. Google understands the AGO's investigation relates to the collection and use of location information, and specifically, via the Google Account settings Location History and Web & App Activity. Google does not understand, and the AGO has not provided any guidance, regarding any nexus of revenue from Android mobile devices and location information.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial relevancy objection and reasserts the other objections made. As previously stated, Google does not maintain such documents in the ordinary course of business. We are currently attempting to ascertain whether this information can be determined through other means. We will update you on our progress.

THIRD SUPPLEMENTAL RESPONSE (Sept. 4, 2019): Google is producing documents Bates-stamped GOOG-GLAZ-00001544 to GOOG-GLAZ-00002105. Google does not maintain documents showing revenue received from Android mobile devices in Arizona, including revenue from advertisements displayed to users of Android devices in Arizona. Google therefore is producing financial statements from 2014 to 2018 that show revenue from all Google products and services, including for Android mobile devices and from advertising. These financial statements identify total revenues as follows: $65,674,000,000 in 2014, $75,544,000,000 in 2015, $89,984,000,000 in 2016, $110,378,000,000 in 2017, and $136,224,000,000 in 2018. In addition, Google remains in the process of determining whether it can provide other information responsive to this request.

FOURTH SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google has not identified documents maintained in the ordinary course of business that reflect revenue on a state level. In order to satisfy the Attorney General's request for information, Google has made an effort to estimate revenue for Arizona relating to mobile devices using Android OS by using nationwide data for Search Ads shown on Google.com for the period of January 1, 2014 - June 30, 2019. That estimate is [redacted]

FINAL RESPONSE:
In your letter dated January 17, 2020, you asked Google to answer the following:

1. Which Google employees were involved in collecting or compiling this data? Please also identify their titles.

- [redacted]

2. Please explain where Google's figures are derived from. For example, from which documents, repositories or other systems was this data collected?

[redacted]

3. What does "Search Ads shown on Google.com" mean? For example, does it include only those ads shown on searches done via Google.com? Does it include searches via other points of entry? Does it include searches done on mobile, desktop, and tablet?

"Search Ads shown on Google.com" are ads that appear on the Google Search Results page on Google.com. This Request for Production asked about Android mobile devices, so Google limited its response to Android mobile devices.

4. Please provide a breakdown of the estimate by year since 2014.

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

REQUEST FOR PRODUCTION NO. 20
Produce documents sufficient to show the revenue Google received from the use by consumers of Google Accounts and of Google-authored apps or Google websites on iOS

devices in Arizona, including revenue from advertisements displayed to such users when using iOS devices during the relevant time period.

INITIAL RESPONSE (April 17, 2019): Google objects to this Request for Production as Google does not maintain this information in the ordinary course of business categorized by U.S. state. Preparing such information would be burdensome and difficult. Additionally, Google objects to this Request as seeking information irrelevant to this investigation.

SUPPLEMENTAL RESPONSE (May 30, 2019): Google reasserts its initial relevancy objection, and reasserts the other objections made below. Google understands the AGO's investigation relates to the collection and use of location information, and specifically, via the Google Account settings Location History and Web & App Activity. Google does not understand, and the AGO has not provided any guidance, regarding any nexus of revenue from apps and websites, and location information.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial relevancy objection and reasserts the other objections made. As previously stated, Google does not maintain such documents in the ordinary course of business. We are currently attempting to ascertain whether this information can be determined through other means. We will update you on our progress.

THIRD SUPPLEMENTAL RESPONSE (Sept. 4, 2019): Google is producing documents Bates-stamped GOOG-GLAZ-00001544 to GOOG-GLAZ-00002105. Google does not maintain documents showing revenue received from the use by consumers of Google Accounts and of Google-authored apps or Google websites on iOS devices in Arizona, including revenue from advertisements displayed to such users when using iOS devices. Google therefore is producing financial statements from 2014 to 2018 that show revenue from all Google products and services, including for Google Accounts, Google-authored apps, Google websites on iOS devices, and revenue from advertisements displayed to such users. These financial statements identify total revenues as follows: $65,674,000,000 in 2014, $75,544,000,000 in 2015, $89,984,000,000 in 2016, $110,378,000,000 in 2017, and $136,224,000,000 in 2018. In addition, Google remains in the process of determining whether it can provide other information responsive to this request.

FOURTH SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google has not identified documents maintained in the ordinary course of business that reflect revenue on a state level. In order to satisfy the Attorney General's request for information Google has made an effort to estimate revenue for Arizona relating to mobile devices using iOS by using nationwide data for Search Ads shown on Google.com for the period of January 1, 2014 - June 30, 2019. That estimate is [redacted]

FINAL RESPONSE:
In your letter dated January 17, 2020, you asked Google to answer the following:

1. Which Google employees were involved in collecting or compiling this data? Please also identify their titles.

- [redacted]

2. Please explain where Google's figures are derived from. For example, from which documents, repositories or other systems was this data collected?

[redacted]

3. What does "Search Ads shown on Google.com" mean? For example, does it include only those ads shown on searches done via Google.com? Does it include searches via other points of entry? Does it include searches done on mobile, desktop, and tablet?

"Search Ads shown on Google.com" are ads that appear on the Google Search Results page on Google.com. The numbers provided in this response are for Apple mobile devices (iOS devices).

4. Please provide a breakdown of the estimate by year since 2014.

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

REQUEST FOR PRODUCTION NO. 21
Produce all complaints or inquiries you have received from users in Arizona about your collection, storage, use, or disclosure of user location data or about users' ability to prevent you from doing any of those things and all of your responses regarding the same.

INITIAL RESPONSE (April 17, 2019): Google objects to this Request for Production because the word "location" is a general and widely-used term that will not meaningfully identify specifically relevant documents. Additionally, Google objects to this Request for Production as Google does not

maintain this information in the ordinary course of business categorized by U.S. state. As a consequence, locating such information would be unduly burdensome. Google is willing to meet and confer about an appropriate scope of, and response to, this Request.

SUPPLEMENTAL RESPONSE (May 30, 2019): Subject to and without waiving Google's objections to this Request, Google is conducting a keyword search of its system for storing communications from users. The search and review process is underway, and Google is working to produce these as soon as possible.

SECOND SUPPLEMENTAL RESPONSE (June 20, 2019): Google remains in the process of searching and reviewing for responsive documents. We will supplement this response when we can, and we anticipate doing so by June 28, 2019.

FINAL RESPONSE:
On June 27, 2019, Google produced responsive information found after a diligent search in documents Bates-stamped GOOG-GLAZ-00001480 - GOOG-GLAZ-00001507. Based on that search, Google has produced responsive documents and has not identified further responsive documents.

GOOGLE'S RESPONSES TO AGO'S SECOND CID

I. DEMANDS FOR INFORMATION

DEMAND FOR INFORMATION NO. 1
To the best of your knowledge and belief, are you producing or otherwise making available for examination with your response to this Civil Investigative Demand all non-privileged documents responsive to numbers 1–2 of the Requests to Produce Documents, below, that are in your possession, custody, or control?

FINAL RESPONSE:
As further described below, yes, to the best of Google's knowledge and belief, it produced all non-privileged and responsive documents.

Regarding Request for Production No. 1, on June 20, 2019, Google produced documents Bates-stamped GOOG-GLAZ-00000951 to GOOG-GLAZ-00001058, containing the written testimony and responses to Questions for the Record submitted by its [redacted] and [redacted], including all exhibits and attachments thereto. Google confirms that no other non-privileged materials within the scope described above were submitted to Congress in connection with the hearings on September 26, 2018, and December 11, 2018.

Regarding Request for Production No. 2, in its June 20, 2019 response, Google objected, stating that the documents selected by counsel and reviewed by Mr. [redacted] and Mr [redacted] in preparation for their testimonies are protected by attorney-client privilege and/or the work-product doctrine and, on these grounds, Google did not produce documents responsive to the request.

DEMAND FOR INFORMATION NO. 2
To the extent that your answer to demand 1 is not an unequivocal "yes," are the reasons why all non-privileged, responsive documents in your possession, custody, or control are not being collected and produced set forth in the response to each request in accordance with the instructions?

FINAL RESPONSE:
Please see Google's response to Demand for Information No. 1. Based on our understanding of this Request for Production, Google has no additional information to provide related to it.

II. REQUESTS TO PRODUCE DOCUMENTS

REQUEST FOR PRODUCTION NO. 1

Produce all documents relating to consumer location tracking or location-data collection, storage, or dissemination by Google or by third-parties that were shared with Congress, any house of Congress, any committee or subcommittee of Congress, any senator or member of Congress, or any congressional staff before or after the Senate Commerce, Science, and Transportation Committee hearing on September 26, 2018 or the House Judiciary Committee hearing on December 11, 2018. This includes but is not limited to any such documents provided, shown, read, referenced, or summarized, in whole or in part, to any senators or members of Congress or staff on Google's own initiative or in response to any formal or informal request; the written testimony submitted by [redacted] and [redacted] including all exhibits and attachments thereto; and the written responses to committee members' or staff's questions submitted before or after the hearings, including all exhibits and attachments thereto.

INITIAL RESPONSE (May 30, 2019): Google objects to this Request for Production because the hearings held before the Senate Commerce, Science, and Transportation Committee on September 26, 2018, and the House Judiciary Committee on December 11, 2018, did not focus on consumer location tracking or location-data collection, storage, or dissemination by Google or by third parties.

Subject to and without waiving its objections, Google is producing, Bates-stamped as GOOG-GLAZ-00000951 to GOOG-GLAZ-00001058, the written testimony and responses to Questions for the Record submitted by its [redacted] and [redacted], including all exhibits and attachments thereto. We are in the process of confirming that no other non-confidential materials within the scope described above were submitted to Congress in connection with the hearings on September 26, 2018, and December 11, 2018.

SUPPLEMENTAL RESPONSE (June 20, 2019): Google has conducted a diligent search for and previously produced all responsive documents regarding this Request for Production.

FINAL RESPONSE:

Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 2

Produce all documents relating to consumer location tracking or location-data collection, storage, or dissemination by Google or by third-parties that were referenced, reviewed, or relied on in preparing for or providing Google [redacted] testimony before the Senate Commerce, Science, and Transportation Committee hearing on September

26, 2018 or Google [redacted] testimony before the House Judiciary Committee hearing on December 11, 2018.

INITIAL RESPONSE (May 30, 2019): Google objects to this Request for Production on the grounds that the documents selected by counsel and reviewed by Mr. [redacted] and Mr. [redacted] in preparation for their testimonies are protected by attorney-client privilege and/or the work-product doctrine and, on these grounds, will not produce documents responsive to this request. *See State ex rel. Corbin v. Ybarra*, 161 Ariz. 188, 192 (1989) (citing with approval *United States v. Noble*, 422 U.S. 225, 238 (19785)), which recognized that "societal interests were far better served when attorneys have the opportunity for 'thorough preparation and presentation of each side of the case'"); *see also* 1 Testimonial Privileges § 2.5 (3d ed. 2017) ("Most courts recognize that when an attorney exercises professional skill in compiling selected documents while preparing the client's case, the documents (as compiled) reflect the attorney's mental impressions and should be afforded work product protection.").

SUPPLEMENTAL RESPONSE (June 20, 2019): Google reasserts its initial objections made below.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

GOOGLE'S RESPONSES TO AGO'S THIRD CID

I. DEMANDS FOR INFORMATION

DEMAND FOR INFORMATION NO. 1

Describe the path that User Location Data takes, beginning with the initial collection by device sensors (i.e., "below" the stack (7/11/19 [redacted] EUO Rough Tr. at 81:13-83:23)), and ending with storage in Sensor Vault, and identify all instances where the location data is "stored" by Google in any form. Identify documents sufficient to confirm the information provided in your response.

INITIAL RESPONSE (Sept. 4, 2019): As Google has described in prior written responses, for a user who enables Location History, a distinct and opt-in Google Account setting, the user has asked Google to save a private map of where the user goes with his or her signed-in devices. As requested, Google's response to this Request focuses on the path of data stored in Sensorvault when a user enables Location History.

This response describes an example of a data path to illustrate as a general matter the way collection, transmission, and storage can occur. This example is therefore not intended as a comprehensive description of every possible path that data could take on a device to Sensorvault. Providing that detailed of a response is not possible given the variety of combinations of device settings and user choices about settings. If the AGO has other examples about which it is interested, Google is willing to meet and confer about providing further information.

[redacted]

[3] As Google explained in previous responses, users can opt any device out of reporting to Location History.



Location History data is stored with these major repositories:

1. Sensorvault (previously Placevault): the history of lat/long locations and associated sensors with users that opted in to Location History.
2. Semantic database: this is a layer of semantic inference data on top of the raw Sensorvault data. This simply means that the data has been given a semantic description, such as "McDonald's" for a place, or "driving on (example road)" for activity segments. This makes locations more user-friendly and understandable than geo coordinates, for example.
3. [redacted]

Internal Google product teams can seek permission to access the data described above, and depending on the use of the data, may access and/or store location information. Any team that needs to store the Location History tied to an individual user is required to respect user deletion choices.

[4] Google Location Services stores a short-term record of the device's query for its location; this record is not associated with the user's Google Account.

FINAL RESPONSE:

Your January 17 Letter asks Google to supplement its previous responses by describing additional paths user location information takes. Specifically, you ask about the following scenarios:

1. Location History on, Location Reporting on, [redacted]/GLA on, battery saver mode off

In order to answer this question, Google is making the following assumptions: (i) the device is running on Android 8, (ii) the device's Location Master toggle is enabled, (iii) "[redacted]/GLA on" and "Battery saver mode off" means the device is in *High Accuracy* mode, and (iv) the user is signed into their Google Account on the device. As the documents Google produced in response to Request for Production 4 of the First CID (e.g., GOOG-GLAZ-00000131) show, when [redacted] had various modes, users could select *High Accuracy*, *Battery Saving*, or *Device only* mode. The disclosure to users explained that Google would improve location accuracy only when users selected *High Accuracy* or *Battery saving* mode. In those modes, the device might use, for example, Wi-Fi and mobile network information to calculate location. In *Device only* mode, the device only calculated location based on GPS.

[redacted]

2. Location History on, Location Reporting on, [redacted]/GLA off, battery saver mode on

As explained above, the documents produced in response to RFP 4 of the First CID (e.g., GOOG-GLAZ-00000131) show that when [redacted] had various modes, users could select *High Accuracy*, *Battery Saving*, or *Device only* mode. The disclosure to users explained that Google would improve location accuracy only when users selected *High Accuracy* or *Battery saving* mode. In those modes, the device might use, for example, Wi-Fi and mobile network information to calculate location. In *Device only* mode, the device only calculated location based on GPS.

Google thus understands this question to be asking about a situation where (i) the device is running on Android 8, (ii) the device's Location Master toggle is enabled, (iii) Battery saving mode is enabled,

and (iv) the user is signed in to their Google Account on the device. This is the same scenario that Google described in its September 4, 2019 response.

3. Location History on, Location Reporting on, [redacted]/GLA off, battery saver mode off

As explained above, the documents produced in response to Request for Production 4 of the First CID (e.g., GOOG-GLAZ-00000131) show that when [redacted] had various modes, users could select *High Accuracy*, *Battery Saving*, or *Device only* mode. The disclosure to users explained that Google would improve location accuracy only when users selected *High Accuracy* or *Battery saving* mode. In those modes, the device might use, for example, Wi-Fi and mobile network information to calculate location. In *Device only* mode, the device only calculated location based on GPS.

Google thus understands this question to be asking about a situation where (i) the device is running on Android 8, (ii) the device's Location Master toggle is enabled, (iii) "[redacted]/GLA off" and "Battery saver mode off" means *Device only* mode is on (where the phone only uses GPS to determine location and [redacted] is not improving location accuracy), and (iv) the user is signed into their Google Account on the device.

[redacted]

2. The user's location information is stored in Sensorvault (previously known as Placevault). The data stored in Sensorvault is not available to third parties. The user can enable Google Location Sharing, which shares the user's location, based on information calculated and available from their Location History, with any person who the user herself designates.

DEMAND FOR INFORMATION NO. 2

Identify all clients, groups, teams or people, internal or external to Google, that have direct access to Location History location data.

INITIAL RESPONSE (Sept. 4, 2019): Access to the Location History data stored in a user's account is limited to internal Google services and products. No parties external to Google have direct access to a user's Location History data.

Any Google teams' access to Location History data is subject to review and compliance with usage policies. To be considered for permission to access Location History data, the team must submit a detailed request that includes information about the Privacy Working Group they work with, their Privacy Design Documents (which are privileged documents created to seek the advice of counsel

advising on the product), and their relevant launch report documentation. The team also must identify their product counsel contact. Additionally, Google requires that the requester seeking access to the data for a specific team and use have a certain level of seniority.

The groups of Google teams that can and do seek approval to access Location History data in Sensorvault are listed below in response to Demand for Information No. 5.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 3
Identify all clients, groups, teams, servers or other subdivisions at Google where User Location Data in any form (whether or not aggregated or anonymized) is stored.

INITIAL RESPONSE (Sept. 4, 2019): Google objects to this request as overly broad and unduly burdensome. Specifically, the term "User Location Data" is overly broad and not within a reasonable definition. As an initial matter, defining "User Location Data" as "data from which a user's location can be determined" suggests that even extremely coarse location information (e.g., country level) could conceivably be included in the definition. Furthermore, including IP address within that definition, when an IP address is needed for any device to connect to and function on the internet, renders this defined term even more unwieldy. Especially when combined with an all inclusive request like this Demand for Information, such a vague term renders the demand prohibitively burdensome.

Notwithstanding this objection, Google provides the following information in an effort to be responsive to this request:

Google previously provided written responses to the First Civil Investigative Demand ("First CID") that described Google Account level location settings.

There are three major repositories that store Location History data: Sensorvault, a semantic database, and [redacted]. These repositories are described in further detail in response to Demand for Information No. 1. Sensorvault stores the location information that a user can share with a third party when the user enables Location Sharing.

The repository that stores users' Web & App Activity data is called [redacted]

Location data that Google saves from the Usage & Diagnostics setting is stored in [redacted] and in corresponding internal logging platforms. It is associated with a user's account for users that have Web & App Activity enabled, as Google explained in response to the First CID. When Usage & Diagnostics data is not associated with a Google user's account because the user does not have the additional Web & App Activity setting (the sub-setting to "Include Chrome history and activity from sites, apps, and devices that use Google services") enabled, the data is not associated with a user's Account in [redacted] and also is stored in Google's internal logging platforms. Both systems have access controls for teams that log and read data from these repositories.

Other Google products and services may receive and store a user's location information, e.g., IP addresses, when a user interacts directly with the product or service from a mobile device. For example, Google's [redacted] team receives and temporarily stores location information when users interact with Google Maps. That team assists in providing geolocation information that enables Google Maps to respond to the user's query to the app. IP address information is needed to operate and offer Google services, and is used for legal compliance and other product operations.

With regard to the request's reference for information about aggregated and/or anonymized location information, Google needs a more detailed understanding of what types of information to which the AGO is referring. Google is willing to meet and confer to determine whether additional information about Google teams' storage of information can be provided.[5]

FINAL RESPONSE:
In Google's February 28, 2019 letter to the AGO and in its first response to the First CID, Google objected to requests to the extent that they were overly broad and unduly burdensome in defining a Relevant Time Period of more than 10 years—January 1, 2007 - present—across such a broad range of products and services. Google explained that in the absence of appropriate limitations, the scope was not manageable and made it difficult for Google to provide useful information in a timely and efficient manner. Subject to and without waiving those objections, Google provided detailed and substantive narrative responses and produced documents.

Specifically, Google's September 4, 2019 response described where location information is stored for Location History, Web & App Activity, and Usage & Diagnostics. Google also explained that other

[5] Google also reiterates its objection to this Demand, and others that reference "aggregated" or "anonymized" data, that such data not associated with a specific user's account is not a proper subject of the Attorney General's investigation under the Arizona Consumer Fraud Act.

products and services may receive and store a user's location information, and mentioned [redacted] as an example.

In addition, as explained above in response to Demand for Information No. 4 of the First CID, Google also produced multiple informative documents on the topic of the storage of location information.

Furthermore, the AGO's Fourth CID asks about 18 additional potential data stores, which Google is in the process of responding to.

Your January 17 letter also asked Google to confirm whether the semantic database is known or referred to by any other name. It is also referred to as [redacted]

Finally, your January 17 letter asked Google to identify where the following information is stored:

- information that is tied to a rotating device ID (see, e.g., [redacted] EUO Tr. page 98)
- Location History data that is used in an "anonymized and aggregated manner" for ads purposes (as described by Google in its response to CID 3, DFI 4)
- anonymized use of Web & App Activity location data (as described by Google in response to CID 3, DFI 8)

For information tied to a rotating device ID, this information is not stored, collectively, in a specific location. Rather, information is stored in the datastore that is specific to the relevant Google product.

For anonymized, aggregated Location History information used for ads (as described by Google in its Response to CID 3, DFI 4), this information is stored in the [redacted] repository. For more information about this repository, please refer to Google's Response to Demand for Information No. 1 of the Third CID.

For anonymized Web & App Activity location information (as described by Google in response to CID 3, DFI 8), this coarsened location information is stored in [redacted] anonymous logs that [redacted]

DEMAND FOR INFORMATION NO. 4
Identify all clients, groups, teams or people, internal or external to Google, that use Location History location data.

INITIAL RESPONSE (Sept. 4, 2019): As we explain in response to Demand for Information No. 2, no parties external to Google have access to or use Location History information that indicates any individual user's location. Each team that has direct access to Location History location data, as explained in response to Demand for Information No. 2, has a process to seek approval and get access to Location History data and is able to use the data for their product or feature implementation in accordance with their user data access request and Google's policies. It is not possible for Google to explain each and every use case, but in response to Demand for Information No. 5, Google has provided examples of how each team that has access to the data uses it.

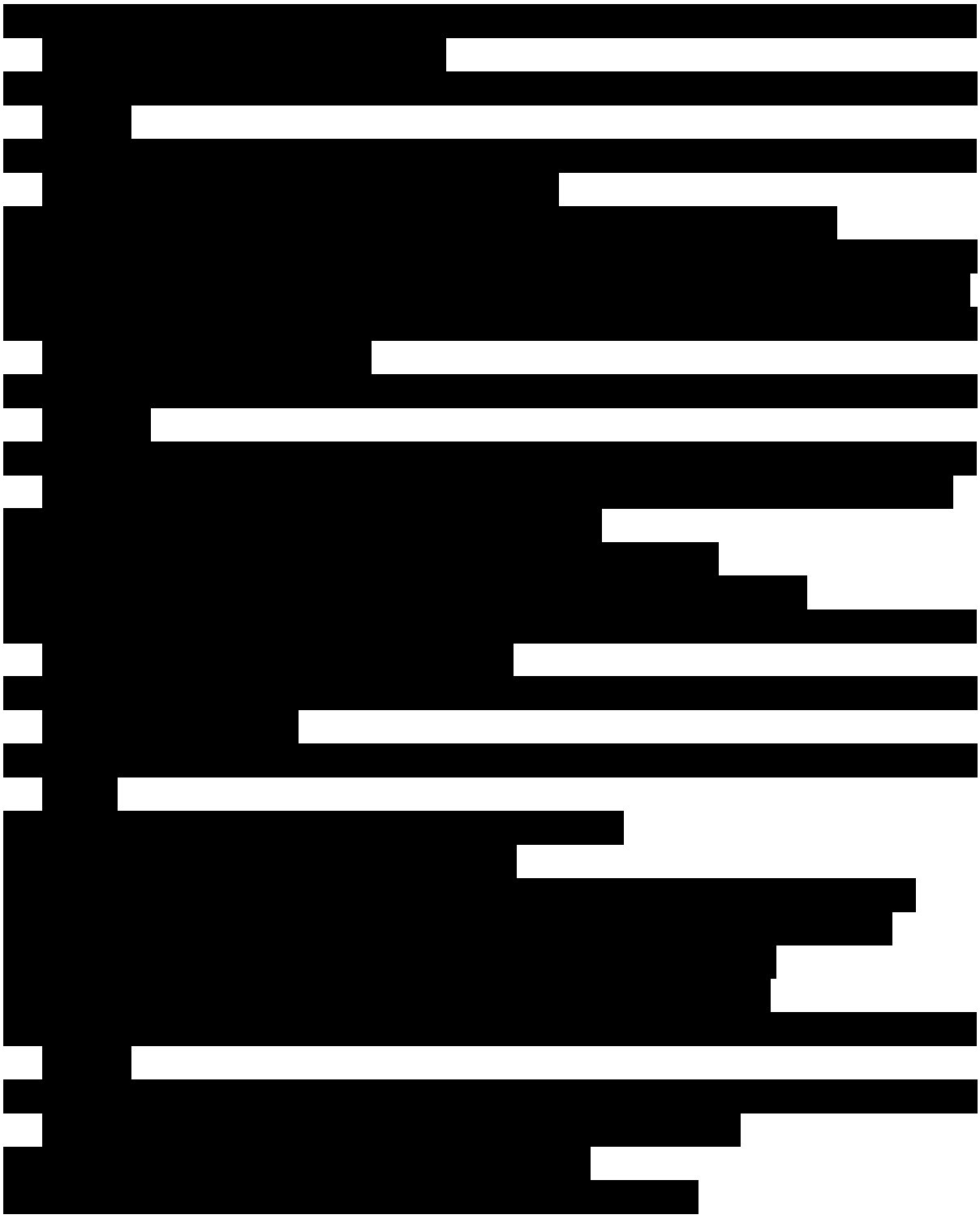
As Google explained in its previous responses to the First CID, Google also uses Location History data in an anonymized and aggregated manner, for users that choose to opt-in to the product, to help advertisers measure how often an online ad campaign helps drive traffic to physical stores or properties. Google does not share any individually identifying Location History information with advertisers. Store visit data cannot be tied to individual ad clicks, viewable impressions, or people.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 5
Identify all approved uses of Location History location data. (See 7/11/19 [redacted] EUO Rough Tr. at 231:10-22).

INITIAL RESPONSE (Sept. 4, 2019): Google provides below teams that had approved uses for Location History information, along with representative examples of each team's use case. It is not practical for Google to identify in a static answer all approved uses given the evolving nature of the work of product teams, which is the reason that Google's Privacy Policy and product-related pages describe broadly the ways in which Google uses data. As we explain in response to Demand for Information No. 1, all teams accessing Location History data must seek approval and must use the data in accordance with Google's policies regarding data access and Google's Privacy Policy.

[redacted]





FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 6
Describe the path that Web & App Activity location data takes, beginning with the initial collection by device sensors, and ending with the location data's storage in Web & App Activity. (See 7/12/19 EUO Rough Tr. at 208:19-210:18).

INITIAL RESPONSE (Sept. 4, 2019): As Google has described in prior written responses, for users who enable Web & App Activity, Google saves the user's activity (e.g., search queries) on Google products and services in the user's Google Account.

The location that is associated with the user's activity on Google products and services is obtained from the device's location services Application Programming Interfaces (API). The device can derive location from sensor data and information about things near a user's device, such as Wi-Fi access points and cell towers, and is provided to the Google products and services via APIs.

If location information is not available from device sensors or otherwise is not part of the user's action (e.g., the user has disabled their device-level location setting), the Web & App Activity entry for that action will not include device-based calculated location. The entry will still include the IP address associated with the user's activity. IP addresses are required for devices to be able to connect to one another through the Internet and are necessary for online services to function.

Below Google sets forth two examples of a path starting with a user's search, which is saved in Web & App Activity. This response is not intended as a comprehensive description of every possible path

that data could take when a user has enabled Web & App Activity. Providing that detailed of a response is not possible given the variety of combinations of device settings and user choices about settings. If the AGO has other examples about which it is interested, Google is willing to meet and confer about providing further information.

The following is an example of a search query for a Google Account with Web & App Activity ON using a device with system location OFF or when device location is otherwise unavailable.



The following is an example search query for a Google Account with Web & App Activity ON using a device with system location ON and the OS location permission ON for the Google App.



FINAL RESPONSE:
Your January 17 letter asked Google to respond to the following questions:

1. To which settings do "system location" and "OS location permission" refer?

"System location" refers to, for example, Google Location Services on a Google-licensed Android device. "OS location permission" refers to, for example, the Location Master toggle on a Google-licensed Android device.

2. Does the term "devices location services API" refer to the Fused Location Provider API? If not, to which API(s) does it refer?

This example was meant to be device agnostic. Thus, the APIs used on iOS devices may be different than APIs used on Android devices. For Google-licensed Android devices, Fused Location Provider is an API that provides location to apps and services with the requisite user permission.

3. What is intended by the term "Google servers," and are these the same servers referenced by Mr. [redacted] See [redacted] EUO Tr. at 218:15–220:6.

"Google servers" as used by Mr. [redacted] refers, generically, to any Google web service that a user may connect to through, for example, the Internet or an app.

4. What is intended by the term "device sensors"?

"Device sensors" has the same meaning as that which Ms. [redacted] used. Device sensors also are explained more in Google's Response to DFI No. 2 of the First CID.

DEMAND FOR INFORMATION NO. 7
Identify all clients, groups, teams or people, internal or external to Google, who have direct access to Web & App Activity location data. (See 7/12/19 [redacted] EUO Rough Tr. at 121:20-123:10).

INITIAL RESPONSE (Sept. 4, 2019): Access to information stored in a user's Web & App Activity is limited to internal Google services, and such access is subject to review and must be in compliance with policy. No parties external to Google have direct access to a user's Web & App Activity data.

As Google explains in its Privacy Policy (available at https://policies.google.com/privacy) and in additional disclosures on the page titled How Google Uses Location Information (available at https://policies.google.com/technologies/location-data and produced in documents Bates-stamped GOOG-GLAZ-00002725 - GOOG-GLAZ-00002727, GOOG-GLAZ-00002734 - GOOG-GLAZ-00002782, and GOOG-GLAZ-00002794 - GOOG-GLAZ-00002811), Google may store user information for use across Google's products and services. Web & App Activity data is specifically used to help Google give users more personalized experiences across Google services. This includes things like faster searches, better recommendations, and useful ads, both on and off Google. In order to provide this personalization to users, various teams at Google use Web & App Activity data for as long as the user chooses to keep it associated with their account.

One type of data that Web & App Activity stores is coarsened device-based location data saved from a user's interactions with Google Search, Maps, and Assistant. According to Google's policies, teams may only access data that they use. So, while teams using a user's past searches to personalize search results would be able to view the coarsened device-based location data in Web & App Activity, they would not access that location data unless they had a use case permitted by Google's policies, examples of which we explain in response to Demand for Information No. 8.

Given Web & App Activity is used by many teams to improve Google users' experiences across Google products and services, in the time provided to respond to this Demand for Information, Google was not able to identify a mechanism to list all teams that can access Web & App Activity data generally. Google is in the process of determining if there is a mechanism to do so and will keep you updated on its progress.

SUPPLEMENTAL RESPONSE (Jan. 17, 2020): Please see Google's response to Demand for Information No. 8, which explains examples of authorized uses for which certain teams accessed device-based Web & App Activity location data. As Google previously explained, various teams at Google are able to view Web & App Activity data, to use it in compliance with Google's policies for permitted use cases.

FINAL RESPONSE:
Google responded to this demand on December 31, 2019, and January 17, 2020. Additionally, Google produced documents responsive to this DFI on February 14, 2020, at GOOG-GLAZ-00203130 - GOOG-GLAZ-00203442.

DEMAND FOR INFORMATION NO. 8

Identify all clients, groups, teams or people, internal or external to Google, that make use of Web & App Activity location data.

INITIAL RESPONSE (Sept. 4, 2019): As we explain in response to Demand for Information No. 7, no parties external to Google have access to or use location information stored in Web & App Activity. Per Google's policies, all internal clients that want to use the device-based location data saved in Web & App Activity must seek approval for their product or feature implementation.

To accurately respond to this request and verify which teams are in fact using Web & App activity device-based location data, Google needs to query data sources including logs, which it was not possible to do in the time provided to respond. Google is in the process of working on this request and will keep you updated on its progress.

There are generally three types of uses for which teams use device-based location from Web & App Activity. The first is to display to users their Web & App Activity in their Google Account and allow users to edit and manage that data. The second use case is to get location for a user at the time of a user's interaction with a Google product or service in order to deliver a more relevant and personalized experience. An example might be a user searching for "weather in Paris" followed by "things to do" where Google would infer that the user means "things to do in Paris." This data may also be used to show the user more relevant ads. The third use of the data is related to product development, improvement, or analysis. This could include, for example, using data at an aggregated level for the query "restaurants near me" to improve search results for users in a given area.

SUPPLEMENTAL RESPONSE (Jan. 17, 2020): Based on a query of Google's systems, the following is a representative list of teams with access to and their use of device-based Web & App Activity location data:



[redacted]

FINAL RESPONSE:
Google responded to this demand on December 31, 2019, and January 17, 2020. Additionally, Google produced documents responsive to this DFI on February 14, 2020.

DEMAND FOR INFORMATION NO. 9
Identify all approved uses of Web & App Activity location data. (See 7/12/19 [redacted] EUO Rough Tr. at 122:2-123:10).

INITIAL RESPONSE (Sept. 4, 2019): It is not possible for Google to explain each and every use case of Web & App Activity device-based location data. Google has provided three examples of the uses for WAA data as part of its response to Demand for Information 8. In order to respond to Demand for Information No. 8, Google is working to identify teams that use Web & App Activity device-based location. If Google is able to do so, Google will provide representative examples of the ways in which the teams use the data in response to the current demand.

SUPPLEMENTAL RESPONSE (Jan. 17, 2020): Please see Google's response to Demand for Information No. 8, which explains examples of authorized uses for which certain teams accessed device-based Web & App Activity location data.

FINAL RESPONSE:
Google responded to this demand on December 31, 2019, and January 17, 2020. Additionally, Google is producing documents Bates-stamped produced documents responsive to this DFI on February 14, 2020.

DEMAND FOR INFORMATION NO. 10
Identify any and all other means Google uses to collect, store, transmit, use, delete or disclose User Location Data outside of Location History and Web & App Activity.

INITIAL RESPONSE (Sept. 4, 2019): Google objects to this request as overly broad and unduly burdensome. Specifically, the term "User Location Data" is overly broad and not within a reasonable

definition. As an initial matter, defining "User Location Data" as "data from which a user's location can be determined" suggests that even extremely coarse location information (e.g., country level) could conceivably be included in the definition. Furthermore, including IP address within that definition, when an IP address is needed for any device to connect to and function on the internet, renders this defined term even more unwieldy. Especially when combined with an all inclusive request like this Demand for Information, such a vague term renders the demand prohibitively burdensome.

Google is making a good-faith effort to respond by providing information about how its suite of GMS products collect, store, transmit, use, delete, and disclose location information, as the AGO has specifically inquired about these services in Request for Production No. 5:

As Google explains in its Privacy Policy (available at https://policies.google.com/privacy), in additional disclosures on the page titled How Google Uses Location Information (available at https://policies.google.com/technologies/location-data and produced in documents Bates-stamped GOOG-GLAZ-00002725 - GOOG-GLAZ-00002727, GOOG-GLAZ-00002734 - GOOG-GLAZ-00002782, and GOOG-GLAZ-00002794 - GOOG-GLAZ-00002811), Google collects, stores, and uses a number of categories of location information.

Collection

Google may collect location information in the following general ways:

IP Addresses

Every device connected to the Internet is assigned an IP address and these numbers are usually assigned in geographic blocks. Thus, an IP address can often be used to identify the location from which a device is connecting to the Internet. IP addresses are needed to operate and offer Google services, including for legal compliance and other product operations.

User Provided Information

Users may provide Google with billing address information or address delivery information in a number of Google products and services. In addition, when users create a Google Account, they may (but are not required to) provide an address. Users may also provide phone numbers associated with their Google account, the area code of which may infer a user's location. In certain products, such as Maps, users may input a home or work address. Finally, users provide information to Google when they enter queries on Search or Maps such as "restaurants near me."

Device Sensors

A number of Google products and services can request access to device-based location, as calculated and provided by the device. As Google explained in its response dated April 17, 2019, to Demand for Information No. 7 of the First CID, Google Location Accuracy (formerly known as Google Location Services) ("GLA") is a network-based location service that collects data to improve location accuracy and provide certain location information to the apps and services with the requisite permissions. The information Google collects from GLA is linked to a temporary and rotating device identifier that is not used by or shared with other services. It is not connected with any identifier that would associate that data with a specific user.

Below we explain how the GMS products may collect location information.

Google
Google may collect search terms associated with a user's search, which may allow Google to infer a user's location. In addition, Google Search may request device-based location.

Chrome Browser
The Chrome browser can request access to device-based location.

Gmail
Gmail may collect user location information from messages, for example, in order to create a calendar entry for an upcoming event (e.g. dinner reservation at [example]). In addition, Gmail will have location metadata associated with certain attachments like photos or videos. As part of the Gmail/Google Account creation process, users may also provide an address to associate with their account.

Google Maps
Maps can collect various location information such as users' queries, device-based location for providing navigation directions, or the location of manual entries that users may save such as their home/work addresses or favorite/saved locations. Maps may also collect location information from other Google products to provide a more personalized user experience. For example, a user's upcoming reservation sent in a Gmail message may display on their Google Maps.

YouTube
The YouTube service may request access to device-based location.

Google Play Store
As a commercial service, Google Play collects user/developer billing information. Play also requests access to device-based location.

Drive
Google Drive stores users' files in the cloud. To the extent that the files contain user location information, for example the metadata associated with a photo, Drive has that information saved for the user.

Google Play Music
As a commercial service, Google Play Music may collect user/artist billing information. Play Music may also request access to device-based location.

Google Play Movies
As a commercial service, Google Play Movies may collect user/artist billing information. Play Movies may also request access to device-based location.

[redacted]
As a video-calling app, [redacted] may collect location information based on phone numbers.

Google Photos
Google Photos may collect geolocation EXIF data from any uploaded photos.

Usage

Google
This app uses location information to provide users with more personalized and relevant search results. This helps Google respond to queries like "restaurants near me."

Chrome Browser
The Chrome browser will allow sites to access the user's location for a number of reasons, including being able to surface relevant content to a user based on location (including for legal obligations -- e.g. users in the EEA must provide consent to websites to use cookies). In addition, the Chrome browser allows users to save addresses for auto-filling and stores location in a way that users can manage (e.g., block certain sites or allow certain sites access to location without having to re-request permission).

Gmail
Gmail may use the location data from messages to populate other Google products with personalized information for the user. This could include upcoming travel or dining reservations on Calendar and on Google Maps.

Google Maps
As a Geo-focused product, Google Maps uses location in a variety of ways including to show users locations they searched for, to provide navigation, and to personalize and recommend places on a map. Maps also displays to users relevant location information based on things like appointments and reservations that a user may have in Gmail or Calendar.

YouTube
YouTube uses location information, for example, to provide users with localized and personalized results, such as surfacing local artists. In addition, YouTube previously used aggregated and anonymized location data to provide wireless carriers network quality information. YouTube also uses location information to restrict access to content as necessary to comply with legal obligations, for example in licensing agreements.

Google Play Store
The Google Play Store uses location information, for example, to send and receive billing and payment information, provide users with relevant app recommendations, and restrict access to content as necessary to comply with legal obligations, for example in licensing agreements.

Google Drive
Google Drive may use IP addresses to determine which Google Drive server should be used to fulfill a user's request in order to reduce latency and be as expedient as possible.

Google Play Music
Play Music uses location information, for example, to send and receive billing and payment information, provide users with relevant app recommendations, and restrict access to content as necessary to comply with legal obligations, for example in licensing agreements.

Google Play Movies
Play Movies uses location information, for example, to send and receive billing and payment information, provide users with relevant content recommendations, and restrict access to content as necessary to comply with legal obligations, for example in licensing agreements.

[redacted] may use IP address to determine a user's country and check if the service is available there.

Google Photos
Photos uses location information, for example, to help users search for photographs from a particular place, to display the location information to the viewer of the photo, and to recognize famous objects and landmarks in a photo, such as the Statue of Liberty or the Eiffel Tower.

Disclosure

Google
Users conducting searches can see the location that Google Search is using at the bottom of the Google Search Results Page.

Chrome Browser
When the user grants a third-party site permission to access location, the Chrome browser will transmit that location to the site. Users are made aware of this request by a browser pop-up.

Gmail
Gmail allows users to send information to other users, and to the extent that includes location information, this will be transmitted to others.

Google Maps
Maps allows users to choose to share Map locations with others by clicking the "Share" options.

YouTube
As explained above, Google used to provide network quality information to third parties based on aggregated and anonymized YouTube location data.

Google Play Store
When users interact with apps on Google Play, they may grant those apps permission to access their location. In addition, developers may access a user's billing information to complete transactions.

Drive
Google Drive allows users to share files with others. To the extent there is location information associated with or in the file, that information may be viewable to others with whom the user has chosen to share the files.

Google Play Music
Content providers may access a user's billing information to complete transactions.

Google Play Movies
Content providers may access a user's billing information to complete transactions.

[redacted] allows others to see the user's phone number, which can provide information about the user's location.

Google Photos
Users may choose to share images in Google Photos with others who will be able to view the location metadata information of the photograph.

Storage & Deletion

Google
For users that have Web & App Activity enabled, Google saves their search results and associated location information in the users' Google Accounts. Users can delete that data at any time. Google recently introduced a feature to allow users to set the data to auto-delete after 3 or 18 months, or to be retained indefinitely for users to manage and delete when they wish.

Chrome Browser
Chrome History may be saved in a user's Web & App Activity with relevant location information, which the user can edit or delete at any time. Also, users can delete any addresses they have stored in Chrome.

Gmail
Users can delete their Gmail content, including location information, at any time.

Google Maps
Users can delete any of their saved locations in Maps at anytime. In addition, Timeline in Maps provides the user interface to manage and delete Location History. Search queries in Maps are saved in a user's Google Account if the user has Web & App Activity enabled, which the user can manage and delete at anytime.

YouTube
Users cannot delete the aggregated and anonymized network quality information data described above, as that data is not associated with any user.

Google Play Store
Users are able to revoke the location permission for any apps at any time. In addition, users can update their account or billing addresses at any time.

Drive
Users can delete files and their associated location information at any time.

Google Play Music
Users can update their account or billing addresses at any time.

Google Play Movies
Users can update their account or billing addresses at any time.

[redacted] stores a user's phone number which users can update at any time.

Google Photos
Users can delete any of their photos along with the associated location information. Additionally, users can remove access permission to photos that they have chosen to share with others via the sharing functionality, so that those users can no longer see the photo and associated metadata that may include location.

Transmission

Data is routinely transmitted between users and Google when users interact with the Internet and on Google's products and services. Like other data, location data can be transmitted to Google passively (e.g., Google receives an IP address) and actively (e.g., Google asks a user to provide their billing

address as part of a transaction and the user enters the information into a form). If the AGO has particular examples about which it is interested, Google is willing to meet and confer about providing further information.

FINAL RESPONSE:
In Google's February 28, 2019 letter to the AGO and in its first response to the First CID, Google objected to requests to the extent that they were overly broad and unduly burdensome in defining a Relevant Time Period of more than 10 years—January 1, 2007 - present—across such a broad range of products and services. Google explained that in the absence of appropriate limitations, the scope was not manageable and made it difficult for Google to provide useful information in a timely and efficient manner. Subject to and without waiving those objections, Google provided detailed and substantive narrative responses and produced documents.

Additionally, Google made a witness, [redacted] available for examinations under oath, who was prepared to speak about how user location information is collected in connection with Android. Further, as mutually agreed, Google is making a fourth witness available for examination under oath later this month to speak about how user location information is collected in connection with Google-authored apps and Google search through a web browser.

Your January 17 letter asked about Google Play Services. As Ms. [redacted] explained in her deposition, Google Play Services is synonymous with GMS Core, which is comprised of many services. Ms. [redacted] explained that she is responsible for the location services within Google Play Services. (See [redacted] EUO Tr. at 62:23-25). She provided detailed information on how those location services work, including the Fused Location Provider API and the Geofencing API. Google's September 4, 2019 response discussed the Fused Location Provider API, for example.

Your January 17 letter also asked about Google's IP Address objection. As Google has stated, Google collects IP addresses, which the AGO included in its definition of "User Location Data." See, e.g., First Civil Investigative Demand, pg. 6 ("'User location data' means any data from which a user's location can be determined, including but not limited to location information collected through device sensors, GPS, Wi-Fi, Bluetooth, cell towers, and IP addresses."). Google has explained that including IP address within that definition, when an IP address is needed for any device to connect to and function on the internet, renders this defined term unwieldy, especially when combined with an all inclusive request like this Demand for Information. Google cannot answer this request given how expansively the AGO has defined User Location Data.

As your January 17 letter pointed out, Google has made a good-faith effort to respond to this request by explaining its location practices for the GMS products:

- Google
- Chrome Browser
- Gmail
- Google Maps
- YouTube
- Google Play Store
- Drive
- Google Play Music
- Google Play Movies
- [redacted]
- Google Photos

Google is also in the process of responding to the AGO's Fourth CID, which asks about specific additional Google products and services.

DEMAND FOR INFORMATION NO. 11
For each of the means identified in Demand For Information No. 10, identify all clients, groups, teams or people within Google who have direct access to any and all User Location Data collected, stored, transmitted, used, deleted or disclosed by Google.

INITIAL RESPONSE (Sept. 4, 2019): The broad scope of this demand makes it impractical and overly burdensome for Google to identify each team or person across the company who has access to location information. The difficulty in complying with this demand is illustrated by how apps and services interact with a user's mobile device. To the extent that a user is interacting with a Google product on a mobile device, IP address may be collected in order to respond to user requests to the product. For example, if a user seeks directions or wants to identify a location in Google Maps from a mobile device, a request for information is sent directly to Google via the app. When a user sends a request via the app, Google will receive the user's IP address in order to return a response (i.e., to send information back to the app in response to the request).

As Google explains in its Privacy Policy (available at https://policies.google.com/privacy) and in additional disclosures on the page titled How Google Uses Location Information (available at https://policies.google.com/technologies/location-data and produced in documents Bates-stamped GOOG-GLAZ-00002725 - GOOG-GLAZ-00002727, GOOG-GLAZ-00002734 - GOOG-GLAZ-

00002782, and GOOG-GLAZ-00002794 - GOOG-GLAZ-00002811), Google may store user information for use across Google's products and services.

As we describe in response to Demands for Information Nos. 1-9, for users that are signed in to Google and that are using Google's products and services identified in Demand for Information No. 10, Google only stores the associated location data in the user's Google Account using Sensorvault and [redacted] if they have Location History or Web & App Activity, respectively, enabled. The teams that can access and use the data in these repositories are explained above in response to Demands for Information Nos. 1-9.

Google is willing to meet and confer to determine whether additional information about Google teams' access of information can be provided.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 12
For each of the means identified in Demand For Information No. 10, identify all clients, groups, teams or people within Google that use any and all User Location Data collected, stored, transmitted, used, deleted or disclosed by Google.

INITIAL RESPONSE (Sept. 4, 2019): Please see our response to Demand for Information No. 11.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 13
For each of the means identified in Demand For Information No. 10, identify all approved uses of any and all User Location Data collected, stored, transmitted, used, deleted or disclosed by Google.

INITIAL RESPONSE (Sept. 4, 2019): Please see our response to Demand for Information No. 11.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 14
For each of the means identified in Demand For Information No. 10, identify the path that location data takes, beginning with the initial collection by device sensors, and ending with its use or storage by Google.

INITIAL RESPONSE (Sept. 4, 2019): Google objects to this request as overly broad and unduly burdensome. Specifically, the term "User Location Data" is overly broad and not within a reasonable definition. As an initial matter, defining "User Location Data" as "data from which a user's location can be determined" suggests that even extremely coarse location information (e.g., country level) could conceivably be included in the definition. Furthermore, including IP address within that definition, when an IP address is needed for any device to connect to and function on the internet, renders this defined term even more unwieldy. Especially when combined with an all inclusive request like this Demand for Information, such a vague term renders the demand prohibitively burdensome. In response to Demand for Information No. 10, Google has made a good-faith effort to provide a number of examples of how its products and services collect, use, store, transmit, delete and disclose location data.

Despite the overly broad scope of this request, to the extent that the AGO is seeking to understand another path that data takes beyond the specific responses to Demands for Information 1 (Location History) and 6 (Web & App Activity), Google is willing to meet and confer about data paths for location information relating to specific Google products, for example, Google Search or Google Maps.

FINAL RESPONSE:
Google's Response to DFI No. 6 of the Third CID outlines a representative path that location information can take from device to storage in a Google Account for Google Search and Google Maps.

DEMAND FOR INFORMATION NO. 15
Identify the person(s) most knowledgeable about the aggregation and anonymization of User Location Data (e.g., via the "aggregation and anonymization" team (7/11/19 [redacted] EUO Rough Tr. at 236:10-14)) that is collected, transmitted, stored, used, deleted or disclosed via Location History.

INITIAL RESPONSE (Sept. 4, 2019): The person most knowledgeable about the aggregation and anonymization of user location information is [redacted]

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 16
Identify the person(s) most knowledgeable regarding Google's collection, storage, use and transmission of User Location Data, as it relates to each of the following (i) Google Mobile Services, (ii) Google Play Services, (iii) the Android Operating System, (iv) the [redacted] team, (v) Google Maps, (vi) web browser(s) and (vii) any other group (except for Web & App Activity or Location History) involved in collection, storage, use and/or transmission of User Location Data.

INITIAL RESPONSE (Sept. 4, 2019):

(i) Google Mobile Services

As explained in our letter dated August 26, 2019, Google Mobile Services (GMS) is a collection of Google applications and APIs that help support functionality across devices. We are providing information about the specific Google applications that are included in GMS in the United States and that use location information:

- Google
- Chrome
- Gmail
- Maps
- YouTube
- Play Store
- Drive
- Play Music
- Play Movies
- [redacted]
- Photos

The person most knowledgeable regarding Google's collection, storage, use and transmission of user location information, as it relates to these products, is [redacted]

(ii) Google Play Services

Please see response to (i) above.

(iii) the Android Operating System

The person most knowledgeable regarding Google's collection, storage, use, and transmission of user location information, as it relates to the Android Operating System is [redacted]

(iv) the [redacted] team

The person most knowledgeable regarding Google's collection, storage, use and transmission of user location information, as it relates to [redacted] is [redacted]

(v) Google Maps

Please see response to (i) above.

(vi) web browser(s) and (vii) any other group (except for Web & App Activity or Location History)

Please see response to (i) above.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 17
Identify the person(s) most knowledgeable regarding Google's collection, storage, use and transmission of User Location Data company wide, including the collection, storage and/or transmission of User Location Data from one group to another.

INITIAL RESPONSE (Sept. 4, 2019): The person most knowledgeable is [redacted]

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 18
Identify the people, including their titles and groups or teams they are a part of, who were at the meeting referenced in the August 13, 2018 email from [redacted] as reflected in GOOG-GLAZ-00001521 at 1523.

INITIAL RESPONSE (Sept. 4, 2019): Google is unable to confirm this information.

FINAL RESPONSE:
Google inquired of Ms [redacted] and Mr. [redacted] regarding this meeting. Neither has any recollection of the attendees; neither recalls attending the meeting themselves. The invited attendees from Google were: [redacted], and [redacted]. These Googlers are all members of the Communications team.

DEMAND FOR INFORMATION NO. 19
Describe in detail the hierarchical structure of Google's "Geo" product area, including each "component," "team," "product," "product focus" and "service" within Geo. (For reference, see 7/11/19 [redacted] EUO Rough Tr. at 34:7-42:15, 52:8-55:8). Include the person(s) (along with title) who oversees, supervises or is otherwise in charge of each hierarchical level.

INITIAL RESPONSE (Sept. 4, 2019): As [redacted] testified in his July 12, 2019 examination under oath and as Google has explained previously, Google does not have a traditional organizational structure. Google maintains a more informal, organic organizational structure of business components and employees that continuously change (in varying degrees) to meet various demands. Google does not maintain a chart or list identifying the "hierarchical structure of Google's 'Geo' product area." That said, this response identifies several representative examples of the "teams" (and their leaders) within Geo. This response uses "teams" to refer to any subset of Geo. This example is not intended as a comprehensive identification of every single "component," "team," "product," "product focus," and "service" within Geo. Providing such a response is not possible given the numerous informal, organic "teams" within Geo. If the AGO has other examples about which it is interested, Google is willing to meet and confer about providing further information.

"Geo" is a product area within Google that is overseen by [redacted]. Ms. [redacted] is a [redacted] at Google.

"Location Platform" is a team within Geo that is overseen by [redacted] and [redacted]. Mr. [redacted] is a [redacted], and Mr. [redacted] is a [redacted].

"Timeline" is a team within Location Platform that is overseen by [redacted] and [redacted]. Mr. [redacted] is a [redacted] and Mr. [redacted] is a [redacted].

"Location History" is a team within Location Platform that is overseen by [redacted] and [redacted]. Mr. [redacted] is a [redacted], and Mr [redacted] is a [redacted].

"Sensorvault" (previously "Placevault") is a team that serves Location History and that is overseen by [redacted] and [redacted]. Mr. [redacted] is a [redacted], and Mr. [redacted] is a [redacted].

"Inference Layer" is a team within Location History that is overseen by [redacted] and [redacted] Mr. [redacted] is a [redacted], and Mr [redacted] is a [redacted].

"Quality" is a team within the Location Platform that is overseen by [redacted] and [redacted] Mr. [redacted] is a [redacted], and Mr [redacted] is a [redacted].

"IP Geo" is a team within Geo that is overseen by [redacted] and [redacted]. Mr. [redacted] is a [redacted], and Mr [redacted] is a [redacted]

[redacted] is a team within Geo that is overseen by [redacted] and [redacted]. Mr. [redacted] is a [redacted], and Mr. [redacted] is a [redacted].

"Geo product experience" is a team within Geo that is overseen by [redacted]. Mr. [redacted] is a [redacted] at Google.

"Google Maps Mobile" is a team within Google Maps that is overseen by [redacted]. Mr. [redacted] is a [redacted] at Google.

FINAL RESPONSE:
To reiterate, Google does not maintain a formal, static organizational chart. Based on our understanding of this Demand for Information, Google has no additional information to provide

related to it.

DEMAND FOR INFORMATION NO. 20

Describe in detail the hierarchical structure of Google's "Knowledge" product area, including each "component," "team," "product," "product focus" and "service" within Knowledge. (For reference, see 7/12/19 [redacted] EUO Rough Tr. at 39:11-47:20). Include the person(s) (along with title) who oversees, supervises or is otherwise in charge of each hierarchical level.

INITIAL RESPONSE (Sept. 4, 2019): As [redacted] testified in his July 12, 2019 examination under oath and as Google has explained previously, Google does not have a traditional organizational structure. Google maintains a more informal, organic organizational structure of business components and employees that continuously change (in varying degrees) to meet various demands. Google does not maintain a chart or list identifying the "hierarchical structure of Google's 'Knowledge' product area" (now known as "Search & Assistant"). That said, this response identifies several representative examples of the "teams" (and their leaders) within Search & Assistant. This response uses "teams" to refer to any subset of Search & Assistant. This example is not intended as a comprehensive identification of every single "component," "team," "product," "product focus," and "service" within Search & Assistant. Providing such a response is not possible given the numerous informal, organic "teams" within Search & Assistant. If the AGO has other examples about which it is interested, Google is willing to meet and confer about providing further information.

"Search & Assistant" (previously "Knowledge") is a product area within Google that is overseen by [redacted]. Mr [redacted] is a [redacted] at Google.

"Search" is a team within Search & Assistant that is overseen by [redacted]. Mr. [redacted] is a [redacted] at Google.

"Google Assistant" is a team within Search & Assistant that is overseen by [redacted]. Mr. [redacted] is a [redacted] ent at Google.

"Search Platforms" is a team within Search & Assistant that is overseen by [redacted]. Mr. [redacted] is a [redacted] at Google.

"News Content/Proactive Search" is a team within Search & Assistant that is overseen by [redacted] Mr [redacted] is a [redacted] at Google.

"Ranking & Eval Tech Advisors" is a team within Search & Assistant that is overseen by [redacted]. Mr [redacted] is [redacted] at Google.

"Web Search" is a team within Search that is overseen by [redacted] Mr. [redacted] is a [redacted] at Google.

"Image Search" is a team within Search that is overseen by [redacted]. Ms [redacted] is [redacted] at Google.

"Search Logs" is a team within Search that is overseen by [redacted] Ms. [redacted] is a [redacted] at Google.

"Scholar Search" is a team within Search that is overseen by [redacted]. Mr. [redacted] is a [redacted] r at Google.

[redacted] is a team within Search that is overseen by [redacted]. Mr. [redacted] is a [redacted] at Google.

"Research and Machine Intelligence" is a team within Search & Assistant that is overseen by [redacted] Mr. [redacted] is a [redacted] at Google.

"Technical Infrastructure" is a team within Search & Assistant that is overseen by [redacted] Mr. [redacted] is a [redacted] at Google.

FINAL RESPONSE:
To reiterate, Google does not maintain a formal, static organizational chart. Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 21
Describe in detail the hierarchical structure of Google's "Ads" product area, including each "component," "team," "product," "product focus" and "service" within Ads. (For reference, see 7/12/19 [redacted] EUO Rough Tr. at 39:11-47:20). Include the person(s) (along with title) who oversees, supervises or is otherwise in charge of each hierarchical level.

INITIAL RESPONSE (Sept. 4, 2019): As [redacted] testified in his July 12, 2019 examination under oath and as Google has explained previously, Google does not have a traditional organizational structure. Google maintains a more informal, organic organizational structure of business components

and employees that continuously change (in varying degrees) to meet various demands. Google does not maintain a chart or list identifying the "hierarchical structure of Google's 'Ads' product area." That said, this response identifies several representative examples of the "teams" (and their leaders) within Ads. This response uses "teams" to refer to any subset of Ads. This example is not intended as a comprehensive identification of every single "component," "team," "product," "product focus," and "service" within Ads. Providing such a response is not possible given the numerous informal, organic "teams" within Geo. If the AGO has other examples about which it is interested, Google is willing to meet and confer about providing further information.

"Ads" is a product area within Google that is overseen by [redacted]. Mr [redacted] is a [redacted] at Google.

"Display Ads" is a team within Ads that is overseen by [redacted]. Mr. [redacted] is a [redacted] at Google.

"Search Ads" is a team within Ads that is overseen by [redacted]. Mr. [redacted] is a [redacted]r at Google.

"Google Properties & Platforms" is a team within Ads that is overseen by [redacted]. Mr. [redacted]r is a [redacted] at Google.

"Shopping, Travel" is a team within Ads that is overseen by [redacted]. Mr [redacted] is a [redacted] at Google.

"Next Billion Users, Payments" is a team within Ads that is overseen by [redacted]. Mr. [redacted] is a [redacted] at Google.

"Display, Video & Apps" is a team within Ads that is overseen by [redacted]. Ms. [redacted] is a [redacted] at Google.

"Reach User Experience" is a team within Ads that is overseen by [redacted]. Ms. [redacted] is a [redacted] at Google.

"Measurement & Analytics" is a team within Ads that is overseen by [redacted]. Ms. [redacted] is a [redacted] at Google.

FINAL RESPONSE:

To reiterate, Google does not maintain a formal, static organizational chart. Since Google's Initial Response, some of the above information has changed. For example, "Display Ads" is overseen by [redacted] and [redacted], who are both [redacted]. "Shopping, Travel" now is within the "Commerce" organization—rather than Ads. "Display, Video & Apps" now is called "Apps, Video, & Display." "Measurement & Analytics" now is called "Analytics, Insights, and Measurement." And "Ads Privacy and Safety" is a new team within Ads that is overseen by [redacted]. Mr. [redacted] is a [redacted] at Google.
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 22
Describe in detail the change(s) relating to "coarsening," i.e., "making the location appropriate," with respect to User Location Data that is collected, stored, used and/or displayed in Web & App Activity in early 2019. (For reference, see 7/12/19 [redacted] EUO Rough Tr. at 176:18-178:10, 184:9-185:17).

INITIAL RESPONSE (Sept. 4, 2019): We believe that Mr. [redacted] referred to "making the location approximate," and have responded accordingly. For location information associated with a user's activity on Google's Search, Maps, and Assistant products, Google made a privacy-enhancing decision to store less precise location data than the user's device is technically capable of providing (e.g., based on the device-sensors and GPS). In addition, Google took steps to make the previous location data stored in users' Google Accounts more coarse. This change occurred in and around April of 2019.

FINAL RESPONSE:
Though it did improve personalization for users, like more accurate areas of interest, it was determined that precise location did not contribute significant improvement to the use of Web & App Activity location information beyond the previous approximate location precision. Before 2015, device location was coarsened to approximately a neighborhood-sized area with a sufficient number of unique users (e.g., 1,000). When precise location was added in 2015, the location provided by the user's device was stored, which could be a precise lat/lon. In 2019 the device-based Web & App Activity location was moved to a coarser level than it was in 2015, approximately a city-sized area with a sufficient number of unique users (e.g., +1,000). Various teams in Geo, Search, and Ads worked on implementing the changes.

DEMAND FOR INFORMATION NO. 23
Identify and describe all disclosures by Google, or changes to Google's public-facing disclosure documents, relating to "coarsening," i.e., "making the location appropriate," of

User Location Data in Web & App Activity in early 2019. (For reference, see 7/12/19 [redacted] EUO Rough Tr. at 176:18-178:10, 184:9-185:17). Identify responsive documents by Bates number. If there are no documents, state "None."

INITIAL RESPONSE (Sept. 4, 2019): Google has multiple express disclosures to users about how it collects, uses, and saves location information, including specifically in connection the Web & App Activity Google Account feature.

The fact that Google stores location information as part of Web & App Activity is disclosed in many places, including:

Google's Privacy Policy

Google's Privacy Policy (available at https://policies.google.com/privacy?hl=en) expressly tells users that "We collect information about your location when you use our services." The Privacy Policy explains how location is determined with varying degrees of accuracy, explaining the different data that can be collected from devices, user-provided information, and data depending on the user's activity on the device and their selected device and account settings. Each explanation has a link for users to click to learn additional information.

The section on Privacy Controls explains how users "Decide what types of activity [they'd] like saved in [their] account." There is a direct link to Activity Controls, which takes a user to the page where they can review, manage, edit, or delete Web & App Activity Data. In navigating to their Google Account and interacting with their Google Account settings, users would see the type of location data stored in their Account.

The relevant parts of Google's Privacy Policy have not been updated in the timeframe inquired about in this request.

Google's Location Data Policy Page

Google publishes a page titled How Google Uses Location Information (available at https://policies.google.com/technologies/location-data). Google has updated this page from time-to-time to provide users additional information. This page specifically addresses how Google may know a user's location based on the user's activity on Google services and explains that it may be stored in the user's Account, depending on their settings:

"As you use our services, we may infer that you're interested in a place even if your device isn't telling us exactly where you are. For example, if you search for "Cafes in Paris", we may assume that you would like to see places near Paris and show you results of cafes there. Depending on your settings, this type of information may be stored with your account and used as one signal to decide whether you might still be in Paris when you do more searches at a later time."

Google last updated this page in June 2019 (see document Bates-stamped GOOG-GLAZ-00002731 - GOOG-GLAZ-00002733). Google produced versions of this page in prior productions.The prior versions of this page also disclosed that "[Google] may collect and use a few types of location information - depending on the products and features you're using - to provide you with a more useful experience on Google."

Help Center Page

Google's help center page about Web & App Activity (available at https://support.google.com/websearch/answer/54068) explains to users that "When Web & App Activity is on, Google saves information like:

- Searches and other things you do on Google products and services, like Maps
- Your location, language, IP address, referrer, and whether you use a browser or an app
- Ads you click, or things you buy on an advertiser's site
- Information on your device like recent apps or contact names you searched for"

The relevant part of this help center page has not been updated in the timeframe inquired about in this request (see documents Bates-stamped GOOG-GLAZ-00002728 - GOOG-GLAZ-00002730 and GOOG-GLAZ-00002812 - GOOG-GLAZ-00002814).

To be clear, though, deciding to coarsen location information saved in a user's MyActivity based on their Web & App Activity was a privacy-enhancing decision. Google of course considers many obligations when deciding whether to update public-facing documentation. Because Google is constantly seeking to improve and enhance its products and services—especially when it comes to user privacy—not all product changes and features result in such updates. One reason for this is that the change will be apparent to the user as he or she interacts with the product in the normal course. Another reason is that there is no new decision or action required from the user and that an update in that instance might cause "user fatigue" and result in them paying less attention to important communications. Finally, whether an update to public-facing documentation is needed must be

balanced with the challenges of updating text across multiple surfaces and languages and the user benefit of doing this when users have other ways to understand product functionality.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 24
Describe how, whether and the extent to which Google continues to collect, store and use more "precise" User Location Data for purposes other than Web & App Activity, after the "coarsening" changed in early 2019 that was described at the July 12, 2019 EUO of Google through [redacted] (For reference, see 7/12/19 [redacted] EUO Rough Tr. at 176:18-178:10, 184:9-185:17).

INITIAL RESPONSE (Sept. 4, 2019): As Google's Privacy Policy and Location Data Policy Page describe, some location information is not precise and may allow an inference of a user's location, but not the exact location (e.g., a user types in a Search query for "pizza place in Phoenix"). Latitude and longitude information from GPS sensors, which may be collected from a user's device when device location settings are enabled, is more precise location information. A user can disable Web & App Activity (the Google Account setting), and still have enabled device location settings and app settings in order to use Google apps and services like Google Maps.

FINAL RESPONSE:
Google collects, stores, and uses more precise user location information in certain instances besides in relation to Web & App Activity. Android Emergency Location Services (ELS) helps mobile network operators, emergency infrastructure providers, and governments provide more accurate location information to first responders during an emergency. ELS uses the location technologie [redacted]. The location is often more accurate and reliable than cell tower IDs and is calculated by [redacted]. ELS is solely for the use of emergency service providers, and location is sent from the user's device to emergency services only when the user explicitly places an emergency call, either directly or through their mobile network.

Additionally, Google Pay's Tap To Pay contactless payment feature lets users pay merchants for goods and services by using their Android phones. As a part of processing payments, Google may receive the name and location of the merchant at which this service is being used. When made available to

Google, users may review a list of contactless payments they've made in the Google Pay app alongside this location information.

Furthermore, users of Google's Hangouts instant messaging application may choose to send others a message including location information. This location can either be sourced from the device's location services API, or can be a location that the user manually specifies (e.g., the user could search for and attach the location of the Eiffel Tower to a message while physically present in the United States). Locations are not automatically sent to others via this platform, and mentioning a location in one message in a conversation does not automatically append location to all subsequent messages.

DEMAND FOR INFORMATION NO. 25

Describe in detail the change(s) relating to the precision of User Location Data, or otherwise relating to the collection, storage and/or use by Google of User Location Data in Web & App Activity in 2014 or 2015. (For reference, see 7/12/19 [redacted] EUO Rough Tr. at 185:2-11, 186:10-18, 188:24-195:17).

INITIAL RESPONSE (Sept. 4, 2019): In order to provide a more personalized experience to Google users, Google started storing precise device-based location as part of Web & App Activity from users' interactions on Google Search and Google Maps in September of 2015. This change did not affect Google's use of IP addresses which Google had been storing for users with Web & App Activity enabled prior to September 2015. Google also stores precise device-based location data from user's interactions with the Google Assistant in a user's Web & App Activity, if they have the setting enabled.

FINAL RESPONSE:

Please see our Response to Demand for Information No. 22. Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 26

Identify and describe all disclosures by Google, or changes to Google's public-facing disclosure documents, relating to changes in the precision of User Location Data, or otherwise relating to the collection, storage and/or use by Google of User Location Data in Web & App Activity in 2014 or 2015. (For reference, see 7/12/19 [redacted] EUO Rough Tr. at 185:2-11, 186:10-18, 188:24-195:17). Identify responsive documents by Bates number. If there are no documents, state "None."

INITIAL RESPONSE (Sept. 4, 2019): During the relevant timeframe, Google's use and storage of location information as part of a user's activity on Google products and services was disclosed to users in the following ways:

User's Google Account in MyActivity

When Google started saving location in connection with Web & App Activity, users could log in to their Google Account and see the location data being saved. Users could also, of course, manage the setting, and edit and delete any of the associated data.

Google's Privacy Policy

Google's Privacy Policies, as modified and updated throughout the years, explains Google's collection, storage, and use of user data—including the location data. Google is producing the full copies of its Privacy Policies from 2014 and 2015 in documents Bates-stamped GOOG-GLAZ-00002734 - GOOG-GLAZ-00002782 and GOOG-GLAZ-00002794 - GOOG-GLAZ-00002811.

Help Center Page

Google updated its help center page for Web & App Activity (available at https://support.google.com/websearch/answer/54068) to give more detail about the types of user data being stored in a user's account. The update specifically explained that location was saved as part of Web & App Activity. Previously, the help center page already explained to users that IP addresses were being saved. Google is producing the version of the help center page where this disclosure was made.

FINAL RESPONSE:
Google previously produced documents that are responsive to this Demand for Information, including the help center page for Web & App Activity at GOOG-GLAZ-00002812-GOOG-GLAZ-00002814. This page specifically explained that location was saved as part of Web & App Activity. Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 27
Was there any way for a user to know that Google had started collecting finer location data in the Web & App Activity starting in 2014 or 2015, other than by logging into the user's activity feed and comparing past and future collections? If so, describe in detail.

INITIAL RESPONSE (Sept. 4, 2019): Please see our responses to Demands for Information Nos. 23 and 26, which explain ways in which Google disclosed (and continues to disclose) its collection of location data in Web & App Activity, including through the user's Google Account, Google's Privacy Policy, and Google's Web & App Activity help center page.

FINAL RESPONSE:
Based on our understanding of this Demand for Information, Google has no additional information to provide related to it.

DEMAND FOR INFORMATION NO. 28
As part of the set-up for Google Accounts created before 2018, did the user receive any disclosure that Web & App Activity includes User Location Data? Is [sic] so, explain and identify responsive documents.

INITIAL RESPONSE (Sept. 4, 2019): When users create a Google Account, they are presented with disclosures relating to Privacy & Terms that explain Google's Privacy Policy and Terms of Service and that provide a link to both of those documents. As explained above, Google's Privacy Policy expressly discloses to users the data that Google collects—including location data. The Google Account creation flow Privacy & Terms section before 2018 specifically informed users that "When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity - including information like the video you watched, device ODs, IP addresses, cookie data, and location...Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data at My Account (myaccount.google.com)." Google is producing documents Bates-stamped GOOG-GLAZ-00002783 to GOOG-GLAZ-00002793 that show a Google Account creation flow with this language.

FINAL RESPONSE:
As part of the set-up for Google Accounts before 2018, users received disclosures that Google collected location information when the user interacted with Google's products and services, and that, depending on account settings, the data may have been stored in the user's Google Account. Google is producing screenshots of a pre-2018 Google Account set-up in documents Bates-stamped GOOG-GLAZ-00203120 - GOOG-GLAZ-00203129.

II. REQUESTS TO PRODUCE DOCUMENTS

REQUEST FOR PRODUCTION NO. 1

Produce documents sufficient to identify all clients, internal or external to Google, who can access, receive or make use of user location data from Location History.

INITIAL RESPONSE (Sept. 4, 2019): Google does not maintain an existing document stating the information sought by this Request. Google had to query a registry to view information to inform the response to the Demand for Information requesting this information.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 2

Produce the "list of uses that have been approved" as an "appropriate use" of location data from Location History, as described by [redacted] at his July 11, 2019 deposition. (See 7/11/19 [redacted] EUO Rough Tr. at 231:1 0-22).

INITIAL RESPONSE (Sept. 4, 2019): Google does not maintain an existing document stating the information sought by this Request.

Google has a registry that contains the descriptions of the proposed data use cases that teams requesting access to Location History submit, in accordance with Google's user data access policies and Location History team guidance (a privileged document that was prepared by counsel). These access requests are privileged because they are part of a process by which teams solicit and receive legal advice and ultimately approval for the proposed data access and use.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 3

Produce documents sufficient to identify all clients, internal or external to Google, who can access, receive or make use of user location data from Web & App Activity.

INITIAL RESPONSE (Sept. 4, 2019): Google does not maintain an existing document stating the information sought by this Request. Google remains in the process of determining whether it can provide other information responsive to this request.

SUPPLEMENTAL RESPONSE (Jan. 17, 2020): Google does not maintain an existing document stating the teams that can access, receive or make use of Web & App Activity device-based location data. Google had to query its systems in order to respond to the Demands for Information 7 and 8.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 4: Produce document(s) sufficient to show "the complete list of access" to location data coming from, going to or otherwise associated with any Web & App Activity. (See 7/12/19 [redacted] EUO Rough Tr. at 90:18-91 :19).

INITIAL RESPONSE (Sept. 4, 2019): Google does not maintain an existing document stating the information sought by this Request. Google remains in the process of determining whether it can provide other information responsive to this request.

SUPPLEMENTAL RESPONSE (Jan. 17, 2020): Google does not maintain an existing document stating the complete access list to Web & App Activity device-based location data. Google had to query its systems in order to respond to the Demands for Information 7 and 8.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 5
Produce documents sufficient to identify all clients, internal or external to Google, who can access, receive or make use of user location data from Google Mobile Services.

INITIAL RESPONSE (Sept. 4, 2019): Google objects to this request as overly broad and unduly burdensome. Specifically, the term "User Location Data" is overly broad and not within a reasonable definition. As an initial matter, defining "User Location Data" as "data from which a user's location can be determined" suggests that even extremely coarse location information (e.g., country level) could conceivably be included in the definition. Furthermore, including IP address within that definition, when an IP address is needed for any device to connect to and function on the internet, renders this defined term even more unwieldy. Especially when combined with an all inclusive request like this Request for Production, such a vague term renders the demand prohibitively burdensome. In response to Demand for Information No. 10, Google has made a good-faith effort to provide a number of examples of how its GMS products use and share location data. If there are any specific GMS products that the AGO would like additional information about, Google is willing to meet and confer to discuss providing such information.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 6
Produce documents sufficient to identify all clients, internal or external to Google, who can access, receive or make use of user location data from Google Play Services.

INITIAL RESPONSE (Sept. 4, 2019): Google Play is one of the GMS products, so please see our response to Request for Production No. 5, which explains why this request is overbroad and unduly burdensome.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 7
Produce any and all launch documents and similar documents related to the following launches.

a. "[redacted] web view launch"" (see 7/12/19 [redacted] EUO Rough Tr. at 295:6-14);
b. "[redacted] language"" or ""[redacted] text updates"" (see 7/12/19 [redacted] EUO Rough Tr. at 334:17-25);

c. ""Location History and Web and App Activity help center changes and/or [redacted] help center changes"" (see 7/12/19 [redacted] EUO Rough Tr. at 335:23-336:6);
d. ""Account creation change"" or ""account creation update"" (see 7/12/19 [redacted] EUO Rough Tr. at 365:17-366:17);
e. ""Coarsening,"" i.e., ""making the location appropriate"" with respect to user location data that is collected, stored, used and/or displayed by Web & App Activity (see 7/12/19 [redacted] EUO Rough Tr. at 176:18-178:10, 184:9-185:17); and
f. Changes in the precision of user location data in Web & App Activity in 2014 or 2015 (see 7/12/19 [redacted] EUO Rough at 185:2-11, 186:10-18, 188:24-195:17).

INITIAL RESPONSE (Sept. 4, 2019): Google is in the process of collecting and reviewing potentially responsive documents. This Request is particularly difficult to comply with as a practical matter, but we will keep you updated on our progress and expected production date. In addition to being voluminous, these launch reports are stored in a database from which information is not easily exportable in a reviewable and production-ready format. In order to comply with this Request, Google needs to run searches across its launch reports in order to locate potentially responsive information. The reports then need to be extracted from the repository, loaded to the review platform, and reviewed for responsiveness and privilege.

SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google will complete its rolling document production that contains documents responsive to this request by mid-January 2019.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 8
Produce any and all documents, emails, IMs, Google Hangouts threads or other transmissions or communications relating to Project Lance.

INITIAL RESPONSE (Sept. 4, 2019): Google is in the process of collecting and reviewing custodial data sources for potentially responsive material. We will keep you updated on our progress and expected production date.

SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google will complete its rolling document production that contains documents responsive to this request by mid-January, 2019.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 9
Produce any and all documents, emails, IMs, Google Hangouts threads or other transmissions or communications relating to "fixing" location history or other user location data issues as referenced in the August 13, 2018 email from [redacted] in GOOG-GLAZ-00001521 at 1523.

INITIAL RESPONSE (Sept. 4, 2019): Google is in the process of collecting and reviewing custodial data sources for potentially responsive material. We will keep you updated on our progress and expected production date.

SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google will complete its rolling document production that contains documents responsive to this request by mid-January 2019.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 10
Produce any and all documents related to Google's anti-fragmentation requirement for third-party developers/manufacturers who want to have Google-authored apps pre-installed on their devices.

INITIAL RESPONSE (Sept. 4, 2019): Google is producing documents Bates-stamped GOOG-GLAZ-00002106 to GOOG-GLAZ-00002724.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 11: Produce any and all documents, emails, IMs, Google Hangouts threads or other transmissions or communications relating to the document entitled "updated statement for AP LH story" as referenced in the August 13, 2018 email from [redacted] as reflected in GOOG-GLAZ-00001216.

INITIAL RESPONSE (Sept. 4, 2019): Google is in the process of collecting and reviewing custodial data sources for potentially responsive material. We will keep you updated on our progress and expected production date.

SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google will complete its rolling document production that contains documents responsive to this request by mid-January 2019.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 12
Produce the document entitled "updated statement for AP LH story" as referenced in the August 13, 2018 email from [redacted] as reflected in GOOG-GLAZ-00001216.

INITIAL RESPONSE (Sept. 4, 2019): Google produced this document in full at GOOG-GLAZ-00001235 (PROD005).

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 13
Produce the document described as "go[redacted] in the August 17, 2018 email from [redacted] as reflected in GOOG-GLAZ-00001528.

INITIAL RESPONSE (Sept. 4, 2019): Google is withholding production of this document because it is privileged. This document was created by and at the direction of counsel for the purpose of giving legal advice.

FINAL RESPONSE:
Google is providing the following information about the assertion of privilege over the document:

DATE COLLECTED	E-MAIL FROM / AUTHOR / CUSTODIAN	PRIVILEGE DESCRIPTION	PRIVILEGE ASSERTION	REDACTED (YES/NO)
26/08/2019	[redacted]	Draft memorandum containing and reflecting legal advice of [redacted] regarding privacy and policy compliance issues prepared in anticipation of regulatory investigation.	Attorney-Client Communication, Attorney Work Product	No

REQUEST FOR PRODUCTION NO. 14
Produce the document described as "go[redacted] in the August 17, 2018 email from [redacted] as reflected in GOOG-GLAZ-00001528.

INITIAL RESPONSE (Sept. 4, 2019): Google is withholding production of this document because it is privileged. This document was created by and at the direction of counsel for the purpose of giving legal advice.

FINAL RESPONSE:
Google is providing the following information about the assertion of privilege over the document:

DATE COLLECTED	E-MAIL FROM / AUTHOR / CUSTODIAN	PRIVILEGE DESCRIPTION	PRIVILEGE ASSERTION	REDACTED (YES/NO)
26/08/2019	[redacted]	Draft memorandum reflecting legal advice of [redacted]* regarding privacy and policy compliance issues prepared in anticipation of regulatory investigation.	Attorney-Client Communication, Attorney Work Product	No

REQUEST FOR PRODUCTION NO. 15

Produce Google's communications to third-party developers relating to the collection, storage, use, deletion and disclosure of user location data collected by third-party apps running on Android.

INITIAL RESPONSE (Sept. 4, 2019): Google is in the process of collecting and reviewing potentially responsive documents. We will keep you updated on our progress and expected production date.

One reason it is difficult to collect these documents quickly is because there are a number of documents that may be relevant to the request. Further, these communications are stored in a repository that requires backend searching to identify a potentially relevant population of communications. After that identification process, Google needs to collect those documents and load them to the review platform. Then, Google can begin to review for responsiveness.

SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google will complete its rolling document production that contains documents responsive to this request by mid-January 2019.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 16

Produce documents sufficient to show whether and the extent to which Google collects, stores and/or uses any user location data associated with users who are not signed into a Google Account. (See 7/12/19 [redacted] EUO Rough Tr. at 391 :1-5).

INITIAL RESPONSE (Sept. 4, 2019): As Google explains in its Privacy Policy (available at https://policies.google.com/privacy), in additional disclosures on the page titled How Google Uses Location Information (available at https://policies.google.com/technologies/location-data and produced in documents Bates-stamped GOOG-GLAZ-00002725 - GOOG-GLAZ-00002727, GOOG-GLAZ-00002734 - GOOG-GLAZ-00002782, and GOOG-GLAZ-00002794 - GOOG-GLAZ-00002811), Google collects IP addresses. Every device connected to the Internet is assigned an IP address and these numbers are usually assigned in geographic blocks. Thus, an IP address can often be used to identify the location from which a device is connecting to the Internet.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 17
Produce documents sufficient to show how, whether and the extent to which Google collects, stores and/or uses any user location data from activity that was conducted before a user signs into a Google Account. (See 7/12/19 [redacted] EUO Rough Tr. at 391 :25-393:15).

INITIAL RESPONSE (Sept. 4, 2019): As Google explains in its Privacy Policy (available at https://policies.google.com/privacy), in additional disclosures on the page titled How Google Uses Location Information (available at https://policies.google.com/technologies/location-data, and produced in documents Bates-stamped GOOG-GLAZ-00002725 - GOOG-GLAZ-00002727, GOOG-GLAZ-00002734 - GOOG-GLAZ-00002782, and GOOG-GLAZ-00002794 - GOOG-GLAZ-00002811), Google collects IP addresses. Every device connected to the Internet is assigned an IP address and these numbers are usually assigned in geographic blocks. Thus, an IP address can often be used to identify the location from which a device is connecting to the Internet.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 18
All documents relating to the "coarsening," i.e., "making the location appropriate" with respect to user location data that is collected, stored, used and/or displayed in Web & App Activity in early 2019. (For reference, see 7/12/19 [redacted] EUO Rough at 176:18-178:10, 184:9-185:17).

INITIAL RESPONSE (Sept. 4, 2019): Google is in the process of collecting and reviewing potentially responsive documents. Google anticipates that documents that may be responsive to this request may exist in the custodial document population or the launch report document population. Please see our response to Request for Production No. 7 for the reasons why discovery related to the launch reports is time-consuming and difficult. Google will keep you updated on its progress and expected response date.

SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google will complete its rolling document production that contains documents responsive to this request by mid-January 2019.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 19
All documents relating to changes in the precision of user location data, or otherwise relating to the collection, storage and/or use by Google of user location data in Web & App Activity in 2014 or 2015. (For reference, see 7/12/19 [redacted] EUO Rough at 185:2-11, 186:10-18, 188:24-195:17).

INITIAL RESPONSE (Sept. 4, 2019): Google is in the process of collecting and reviewing potentially responsive documents. Google anticipates that documents that may be responsive to this request may exist in the custodial document population or the launch report document population. Please see our response to Request for Production No. 7 for the reasons why discovery related to the launch reports

is time-consuming and difficult. Google will keep you updated on its progress and expected response date.

SUPPLEMENTAL RESPONSE (Dec. 31, 2019): Google will complete its rolling document production that contains documents responsive to this request by mid-January 2019.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

REQUEST FOR PRODUCTION NO. 20
Documents sufficient to confirm your responses to Demand For Information Nos. 1-28.

INITIAL RESPONSE (Sept. 4, 2019): The documents that Google relied on for its responses are noted in each individual response above.

FINAL RESPONSE:
Google completed its rolling production for CIDs 1-3 on February 14, 2020, which contained responsive, non-privileged material from the custodians, date ranges, and search terms previously disclosed to and incorporating feedback from the AGO.

Exhibit 209

From: [redacted]
To: [redacted]
Sent: Mon, 06 Feb 2017 21:02:51 +0000
Subject: Re: user location product excellence
Cc: [redacted]

[redacted]

[redacted]

On Mon, Feb 6, 2017 at 08:53 [redacted] wrote:

[redacted]

[redacted]

--
[redacted]

On 2 February 2017 at 20:00, [redacted] wrote:

On Thu, Feb 2, 2017 at 1:56 PM [redacted] wrote:

> hey [redacted], I'll go ahead and schedule a 1:1 to get some guidance as to how to package all of this discussion in one item that's presentable to [redacted]
> To be clear - Platform Excellence, as I initially conceived of it, is not a Critical User Journey. It's a client-facing excellence fo[redacted] org is in the same boat, so to speak. I think I'll follow that track separately from what the CUJs that [redacted] is our task force is looking at. (unless you guys think we should have a Platform Excellence as an entry in that list and focus on internal "users" a la Geo as a Platform). I didn't get the sense that the task force is particularly passionate about platforms.
>
> I have the same sense. I'm not sure if I have very good ideas about platform excellence either. [redacted]
>
> That said, we have Location as a product umbrella that includes Location History, [redacted] and a bunch of other stuff that's super messy. And it's a Critical User Journey to make sense

out of this mess. This is what I'd like to pursue as part of the task force (and I need help from [redacted] por favor :)).

[redacted]

[redacted]

On Thu, Feb 2, 2017 at 8:55 AM, [redacted] wrote:

[redacted], regarding your last point, what do you feel we should put together as a vehicle for persuasion to the PE task force?

Should it be questions, answers/proposal, or a sad story about our current state?

On Thu, Feb 2, 2017 at 08:52 [redacted] wrote:

Very good points. Thanks for carring about it!

I'm adding [redacted] and [redacted] who have been helping build a robust PE story around user location.

Also, take a look at [redacted] - work in progress, trying to rein in the overall mess that we have with regards to data collection, consent, and storage.

I hope we could land on [redacted] top 5 as "make user location work and make it simple".

On Thu, Feb 2, 2017 at 08:32 [redacted] wrote:

I wrote this note on the main thread with [redacted]

"User location issues. I have trouble framing exactly the CUJ here. I believe users mostly expect that Google knows their precise location when they are using GMM or searching from a mobile device. Yet we often don't know where they are. How can we provide a good location for every user who wants it? How can we be clear and transparent when we don't know precisely where they are? How can we do a great job of respecting people's privacy when they don't want to share their location. Tests: This one feels pretty broad. In fact there's a team in local that has been working across 3 PAs to make progress on the issue."

I think these issues are kind of related to your platform excellence ideas. As I think about it:
- Users expect we know where they are right now almost all of the time.
- Do users with significant privacy concerns understand what data we are saving? Do they know how to control when we store location information?

- Can we have a foreground only model? Lots of users don't care about location history.
- Do users understand how their apps location usage connects to system-settings or resource usage?

Perhaps we should talk about this 1:1 and see if we can figure out how to be most persuasive in the larger task force.

[redacted]

--

[redacted]

--

[redacted]

--

[redacted]

Exhibit 219

Google

ISSUES COVERAGE REPORT
Location History - AP Story Day 4 (shorter report than previous ones)

Wednesday, August 16; 3:30 pm PT

Sentiment | Coverage Themes | Social Conversation | Third Party Commentary | Coverage Links

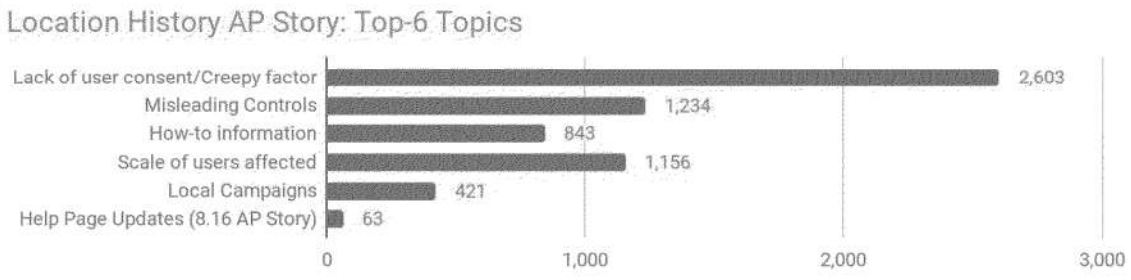
Today, Ryan Nakashima noticed that we posted an update to our Location History Help Center and broke the news (AP NewsBreak: Google clarifies location-tracking policy), that Google revised its help page to clarify that it still tracks user location even if "Location History" is turned off. The AP tweeted the story out, which created a surge of social chatter (~8,000 re-tweets) and the story was picked up by +60 outlets, including The New York Times, U.S. News and World Report and The Washington Post. Both CNET and Axios published original stories, which include brief overviews of the original AP stories that ran on Monday.

SENTIMENT:

MEDIA COVERAGE					
GLOBAL - ALL PUBS / ENGLISH ONLY					
Mentions	**Positive**	**Negative**	**Neutral**	**Social Shares**	**Headlines vs. Mentions vs. Feature Articles**
3,738* (total stories since 2pm 8/16)	**0%**	**100%**	**0%**	**187,007** (including FB shares)	**Headlines: 66% Mentions: 20% Feature Articles: 13%**

** 63 stories (1.69%) are pick-up from today's AP story*

COVERAGE THEMES:



- 69% of coverage mentioned ***the lack of user consent / creepy factor***, including eWeek and Alphr
- 33% of coverage mentioned ***misleading controls***, including Slate and Android Newspad
- 23% of coverage mentioned ***how-to information for consumers managing their data***, including Spyware News and KPEL
- 31% of coverage mentioned ***the scale of the users affected***, including IT Security Guru

Google

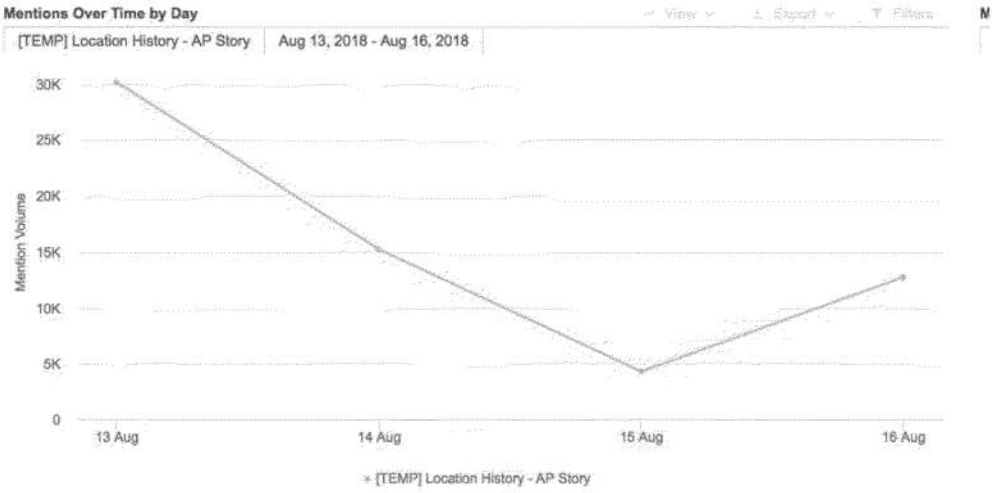
- 11% of coverage mentioned ***Local Campaigns***, including Waynesville Daily Guide (AP pick-up)
- 1.69% of coverage ran as a result of the 8/16 AP story on Google's help page updates, including The New York Times, U.S. News and World Report and The Washington Post

SOCIAL CONVERSATION:

Volume (does not include Facebook):

- VOLUME: **62,000 mentions** since the story broke.
  - Mentions by day still highest on day 1 and trended downward until day 4 (totay) due to new AP reporting.
  - Driven by ~8,000 re-tweets of this AP tweet

Mentions by day.



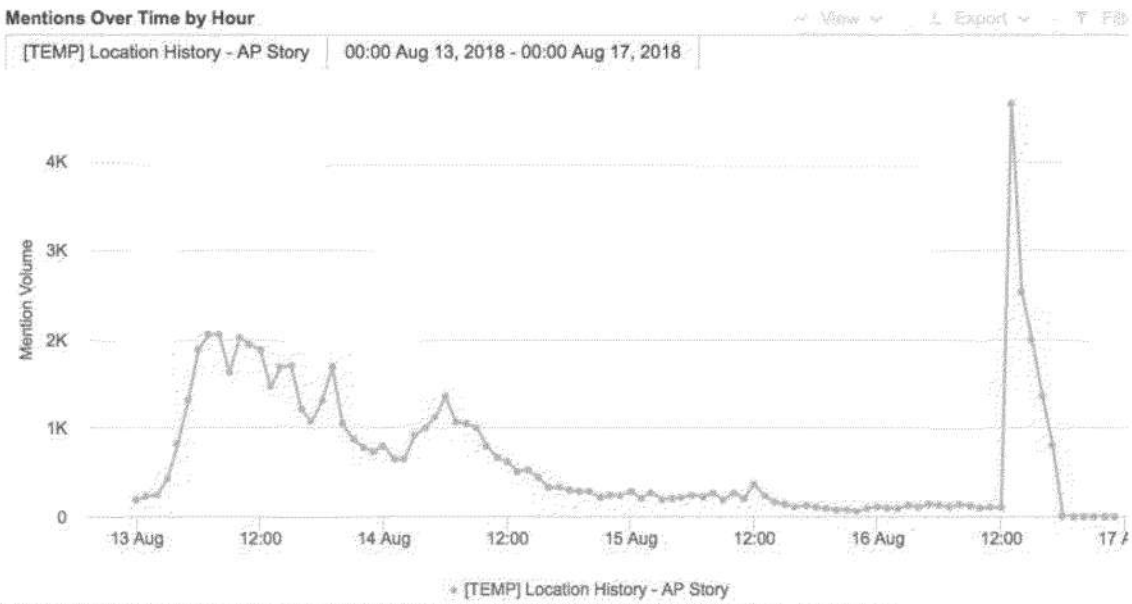
Mentions by hour.

  - CONTEXT: The story peaked TODAY at 1pm PT with more than 4,600 mentions/hour. Day 1 of the story had peaked at 2,000 mentions/hour.
    - For comparison, we saw approximately 2,000 mentions/hour during the peak of the Dragonfly cycle two weeks ago.

TOPICS (today):



Google



Of the 12,711 mentions today, 7,945 of the mentions were retweets of this AP tweet.

- Other engaged tweets came from conservatives:
  - Ryan Saavedra: Does @Google track the location of minors?
  - Mike Cernovich: This is literally fraud, it's time for massive class action lawsuits against Google.https://apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211 …
- Director of Cybersecurity for EFF: When you tell Google to stop tracking your location, it should stop tracking your location. Period.

Full social report here

COVERAGE - UNIQUE GLOBAL:

Full list of global coverage is linked here.

Shared Articles:

- Associated Press: 24,430 shares
- BBC: 11,901 shares
- Hacker News: 7,722 shares
- The Guardian: 6,162 shares
- Today: 4,517 shares
- Global News Canada: 3,709 shares
- Wired: 3,670 shares
- CTV News: 3,415 shares
- Breitbart: 3,414 shares
- CBC: 3,326 shares
- The Guardian: 2,049 shares
- The Hacker News: 1,399 shares
- Alaska Dispatch News: 1,906 shares
- Digital Trends: 1,874 shares
- CNBC: 1,347 shares
- Associated Press: 1,138 shares
- End Time Headlines: 1,127 shares
- CNET: 1,026 shares
- Global News Canada: 935 shares
- CBS News: 922 shares

Google

ISSUES COVERAGE REPORT
Location History - AP Story Day 2

Tuesday, August 14

Sentiment | Coverage Themes | Social Conversation | Third Party Commentary | Coverage Links

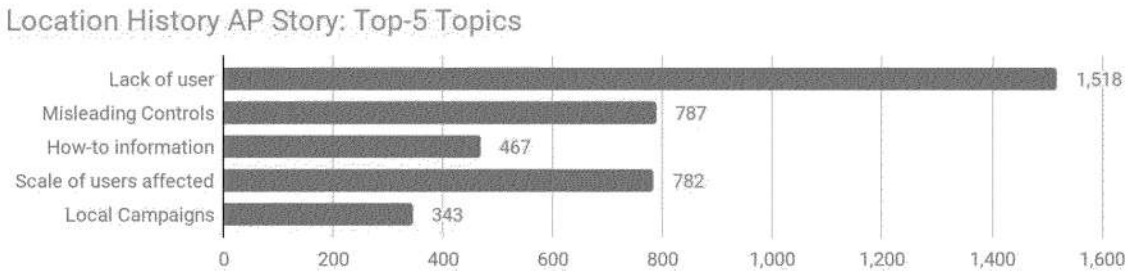
The second day of the AP Location History cycle (AP Exclusive: Google tracks your movements, like it or not and How to find and delete where Google knows you've been) got legs in the UK with negative pieces in the BBC and The Guardian. While the story is trending down (only +430 original articles today), The Today Show extended the consumer cycle around "how you can keep Google from tracking you". Ads mentions slightly increased in volume by 117 stories, but the percent of overall stories that mentioned Local Campaigns decreased from 30% yesterday to 19.2% today, signaling that ads are becoming less of a focus in this narrative. **By the end of the day, this story was no longer on the list of top 10 trending stories across tech.**

We fielded less than 10 press inquiries today, bringing the total to just under 50.

SENTIMENT:

MEDIA COVERAGE					
GLOBAL - ALL PUBS / ENGLISH ONLY					
Mentions	***Positive***	***Negative***	***Neutral***	***Social Shares***	***Headlines vs. Mentions vs. Feature Articles***
1,787 *(total stories since 2pm 8/13)*	*0%*	*100%*	*0%*	***67,170*** *(including FB shares)*	***Headlines: 84.3%*** ***Mentions: 7.2%*** ***Feature Articles: 8.5%***

COVERAGE THEMES:



Although lack of user control continues to trump coverage themes, ads decreases and others remain constant

- 85% of coverage mentioned ***the lack of user consent / creepy factor***, including Quartz, BBC, The Guardian

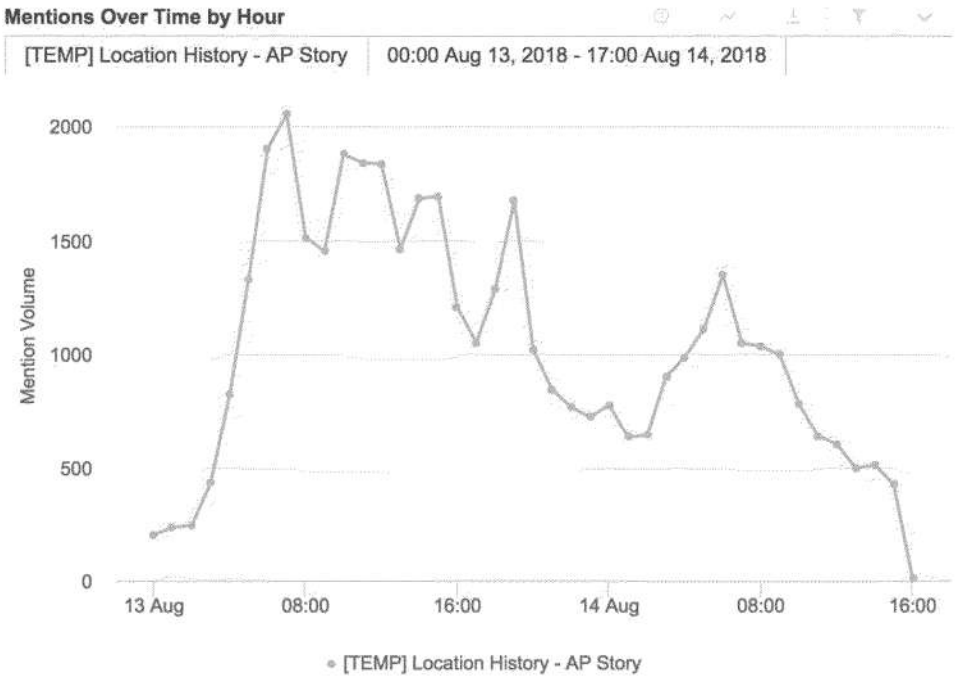
Google

- 44% of coverage mentioned ***misleading controls***, including Android Authority, Mobile Marketing Magazine, Irish Times
- 26% of coverage mentioned ***how-to information for consumers managing their data***, including The Today Show, CNET, Business Insider
- 44% of coverage mentioned ***the scale of the users affected***, including Mirror, TechRepublic, PC Authority
- 19% of coverage mentioned ***Local Campaigns***, including Silicon Republic

SOCIAL CONVERSATION:

Volume (does not include Facebook):

- As of 3:15pm PT on 8/14: **42,000 mentions** over the past two days, peaking at 7-8am PT yesterday with just over 2,000 mentions/hour. Overall, the story is trending downward - there was a spike this morning but volume has decreased every subsequent hour and well into the afternoon (data for 4-5pm PT today has not yet come in so don't misread the "drop" at the end)
- Within this volume, here are the most shared stories (these figures include Facebook shares which our social media listening tool, BrandWatch, cannot include due to privacy restrictions):
  - Most shared articles are from Associated Press (10,595 shares), Hacker News (5,462 shares), The Guardian (4,459 shares), Global News Canada (3,709 shares), Breitbart (3,203 shares), CTV News (2,956 shares), CBC (2,553 shares), and Wired (1,907 shares).



- CONTEXT: For comparison, we saw approximately 2,000 mentions/hour during the peak of the Dragonfly cycle two weeks ago.
- COMPARISON to other hot topics (now looking at Day 2 totals):
  - Dragonfly day 2: 14,400 mentions

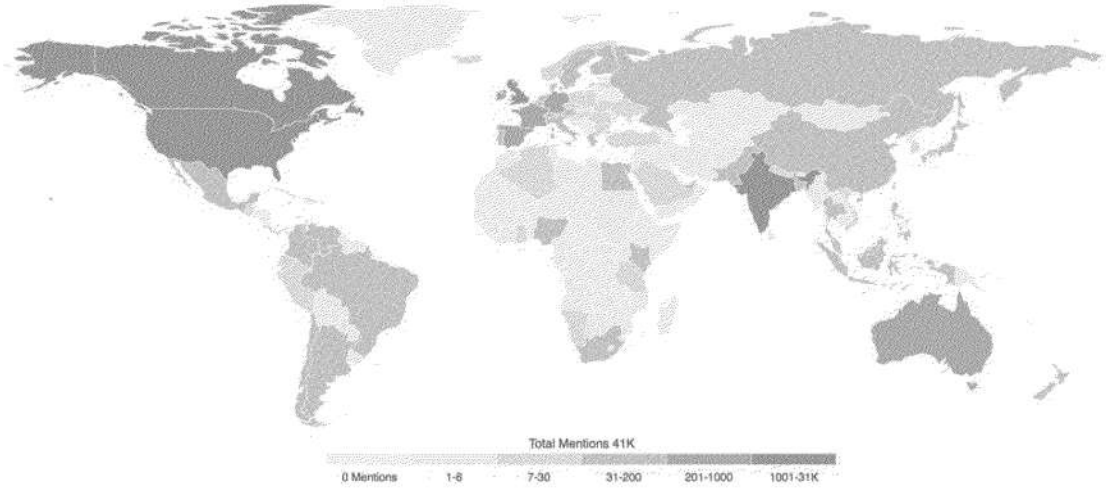
Google

- Gmail API day 2: 6,700 mentions
- YouTube Fake Views day 2: 1,000 mentions
- **Location History day 2 (so far): 15,200 mentions**

Topics (does not include Facebook):



Geography: The USA accounts for 77% of the mentions related to this story.



Includes all social pick up except for Facebook

- MEDIA
  - As of 4pm PT, this story is no longer on the list of top 10 trending stories across tech
  - Yesterday, at its peak, this story accounted for more than half of the top 10 trending tech stories

Google

- NOTABLE TWEETS
  - Sen. Richard Bluemthal: It should be simple—"off" means "off." Google's relentless obsession with following our every movement is encroaching & creepy. I've called for an FTC investigation into its persistent privacy invasions. [link to AP story]
  - Luther Lowe (Yelp): This explosive piece on illicit location tracking by Google has a significant nexus w/Google's abuse of dominance in local search: key source was, "a graduate researcher [who was] ***prompted to rate a shopping trip to Kohl's,*** even though she had turned Location History off." Google desperately wants a foothold in local because 40% of all Google searches have local intent. That's the *plurality of all search* -- 1.5 billion queries per day. Instead of competing on the merits, Google nudges users to read & write reviews that are objectively inferior.
  - Nick Confessore (NYT): Google's explanation of how it discloses location tracking versus what it promised the @FTC it would do. [Refers to tweet below]
    - Justin Brookman (Consumers' Union/former FTC): [see link for images] I turned off Google Location History years ago, but just checked my phone and somehow the setting had been turned back on. □
  - Daniel Stoller (Bloomberg Law): Attorneys have told me today that @Google could face FTC and state-level investigations for the location tracking issue. Google may have followed its privacy policy, but if it isn't clear to the user it could be the basis for regulatory action. FTC declined to comment.
  - Josh Fischman (Scientific American): Map shows unethical #PrivacyInvasion by Google, which tracks your movements when you tell it to stop. https://apnews.com/828aefab64d4411bac257a07c1af0ecb …. Great investigation by @AP.
  - Caitlin Kelly (WIRED): You practically need Google Maps directions to find the settings needed to *actually* stop Google from tracking your location. From @EmilyDreyfuss
  - Nick Short (conservative): Do you have your "location history" turned off? Doesn't matter. Google's still tracking you. [link]
  - Pascal Heyman (Belgian political figure): #Google records your location even when you tell it not to. When is Google (and others)'s massive privacy violation finally going to stop? [link to Guardian story]
  - Luke Rudkowski (conservative): Google tracks your movements, like it or not -- An Associated Press investigation found that many Google services on Android devices and iPhones store your location data even if you've used privacy settings that say they will prevent it from doing so
  - Emily Dreyfuss (WIRED): In light of the @AP's bombshell report on Google Location History, I wrote about how hard it is to find the setting to *actually* turn off your Google location tracking https://www.wired.com/story/google-location-tracking-turn-off/ …
  - Nick Confessore (NYT): How a normal user would expect to turn off Google's location tracking versus the super clear and straightforward way Google does it: [image]
  - Barton Gellman (Princeton): Respectfully note that AP, which published this important privacy story, allows advertisers and data consolidators to track your location and many other things when you visit the site. Including Google. Far from the worst news site, but still.
  - Reed Albergotti (The Information): The AP on Google's location tracking even when people have turned off location tracking. Shouldn't be a surprise when you're using tools created specifically for the purpose of surveillance advertising but it's still interesting.

Google

- Ashkan Soltani (former FTC CTO): This is the confusing privacy dialogue from @google may land another @FTC inquiry. "Even with Location History paused, some Google apps automatically store time-stamped location data without asking."
- The following influential accounts have tweeted a link to associated coverage (not an exhaustive list):
  - Cory Doctorow (writer)
  - Paul Joseph Watson (Info Wars)
  - Mike Cernovich
  - Jack Posobiec
  - Sara Carter (Fox News)
  - Zeynep Tufecki (NYT)
  - Adam Baldwin (actor)
  - Gianni Riotta (journalist)
  - Zeke Miller (AP)
  - Josh Greenman (NY Daily News)
  - Richard Nieva (CNET)
  - Matt Drange (The Information)
  - Kevin Corke (Fox News)
  - Jonathan Lemire (AP)
  - Ryan Heath (Politico)
  - Byron Tau (WSJ)
  - Zack Whittaker (TechCrunch)
  - Justin Hendrix (NYC Media Lab)
  - Jerome Corsi (conservative writer)
  - Morgan Fairchild (actress)

Link to full social report here.

COVERAGE - UNIQUE GLOBAL:

Full list of global coverage is linked here.

Shared Articles:

- Associated Press: 10,595 shares
- Hacker News: 5,462 shares
- The Guardian: 4,459 shares
- Global News Canada: 3,709 shares
- Breitbart: 3,203 shares
- CTV News: 2,956 shares
- CBC: 2,553 shares
- Wired:1,907 shares
- Alaska Dispatch News: 1,906 shares
- Digital Trends: 1,591
- The Hacker News: 1,399 shares
- End Time Headlines: 1,064 shares
- CNBC: 993 shares
- NBC News: 752 shares
- Daily Mail: 705 shares
- Business Insider: 694 shares
- RT: 678 shares
- Western Journal: 656 shares
- CTV News: 649 shares
- The Verge: 612 shares

ISSUES COVERAGE REPORT Day 1

Google

Location History - AP Story

Monday, August 13 (3:00 p.m. PT)

Sentiment | Coverage Themes | Social Conversation | Third Party Commentary | Coverage Links

This morning's Associated Press stories (AP Exclusive: Google tracks your movements, like it or not and How to find and delete where Google knows you've been) about Google's use of user location data resulted in a mix of syndicated stories and original reporting in key online / print outlets including Axios, CNBC, Washington Post, NYT, Fast Company and local outlets. On TV, CBS This Morning and a few local news stations ran stories following the same narrative that Google is tracking your movements regardless of privacy settings and Tucker Carlson from FOX News is expected to cover the story tonight at 8:45pm ET.

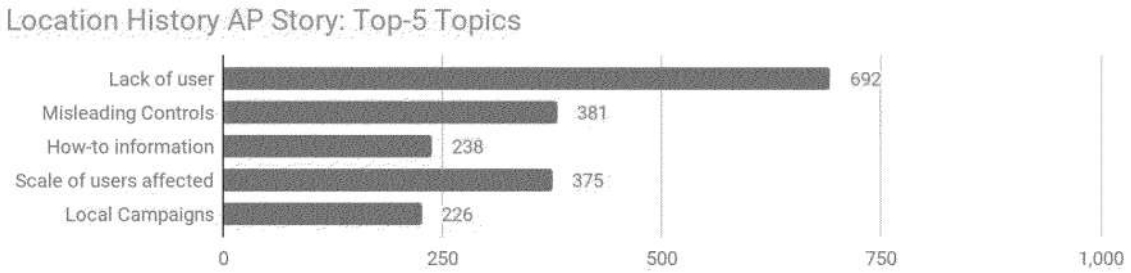
We're seeing a growing narrative driven by third party commentary (policy influencers), that alludes to FTC / congressional action (CNET, Vanity Fair, Wired). This will likely become a bigger focus as the week goes on.

As a result of today's cycle, we have fielded over 40 inbound inquiries. Currently, 51.3% of resulting coverage following the AP report includes our updated statement.

SENTIMENT:

MEDIA COVERAGE					
GLOBAL - ALL PUBS / ENGLISH ONLY					
Mentions	*Positive*	*Negative*	*Neutral*	*Social Shares*	*Headlines vs. Mentions vs. Feature Articles*
741	*0%*	*100%*	*0%*	*5,295*	*Headlines: 94.3% Mentions: 2.9% Feature Articles: 2.8%*

COVERAGE THEMES:



- 93% of coverage mentioned ***the lack of user consent / creepy factor***, including Axios, Bloomberg, Mashable.

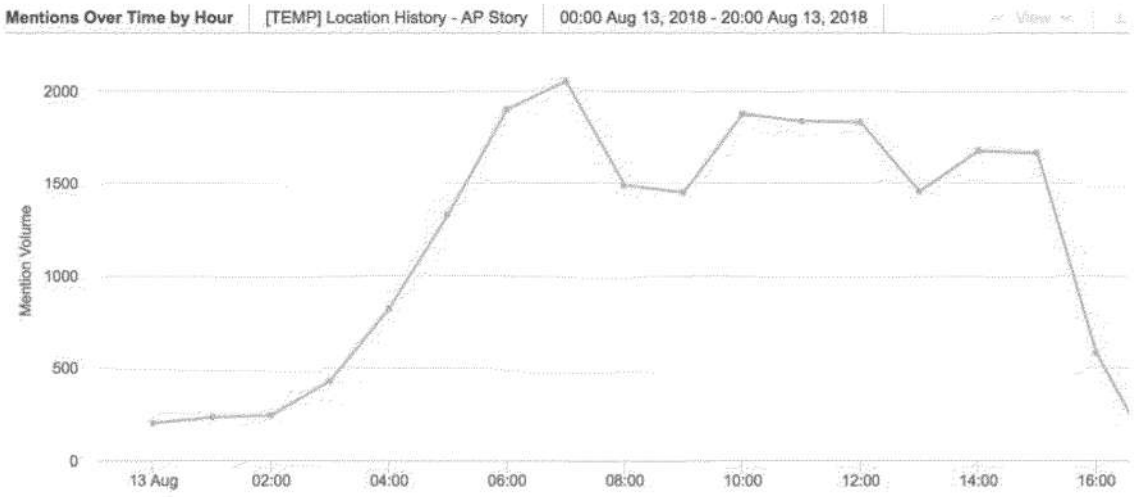
Google

- 51% of coverage mentioned ***misleading controls***, including CNBC, Wired, Consumer Affairs.
- 32% of coverage mentioned ***how-to information for consumers managing their data***, including Gizmodo, Buzzfeed, Mic.
- 51% of coverage mentioned ***the scale of the users affected***, including Associated Press, The Guardian, GQ Magazine.
- 30% of coverage mentioned ***Local Campaigns***, including Vanity Fair.

SOCIAL CONVERSATION:

Volume (does not include Facebook):

- As of 4:15pm PT on 8/13: We've seen approximately. **21,000 mentions** of this story so far today, peaking at 7-8am PT with just over 2,000 mentions. For the past 2 hours, there have been 1,600+ mentions/hr, indicating that this story has continued to trend throughout the day. (Results for 4pm PT update throughout the hour, so do not read into the "drop").
- Within this volume, here are the most shared stories (these figures include Facebook shares which our social media listening tool, BrandWatch, cannot include due to privacy restrictions):
    - Most shared articles are from Associated Press (1,961 shares), CTV News (481 shares), SBS Australia (279 shares) , WRCB-TV Online (200 shares), The Hacker News (118 shares), and NBC News (102 shares).



- CONTEXT: For comparison, we saw approximately 2,000 mentions/hour during the peak of the Dragonfly cycle two weeks ago
- COMPARISON to other hot topics:
    - Dragonfly day 1: 22,000 mentions
    - Gmail API day 1: 3,400 mentions
    - YouTube Fake Views day 1: 2,000 mentions
    - Location History day 1 (so far): 21,000

Topics (does not include Facebook):

Google



Includes all social pick up except for Facebook

- Media Trending Analysis
  - The AP story is still the 5th most trending tech story in past 24 hours (down from 4th two hours ago).
  - Among Google/YouTube stories, versions of the AP story and follow-on coverage are 6 out of the top 10 trending (the top 6 stories)

- NOTABLE TWEETS (nothing notable new since 1pm)
  - Daniel Stoller (Bloomberg Law): Attorneys have told me today that @Google could face FTC and state-level investigations for the location tracking issue. Google may have followed its privacy policy, but if it isn't clear to the user it could be the basis for regulatory action. FTC declined to comment.
  - Josh Fischman (Scientific American): Map shows unethical #PrivacyInvasion by Google, which tracks your movements when you tell it to stop. https://apnews.com/828aefab64d4411bac257a07c1af0ecb …. Great investigation by @AP.
  - Caitlin Kelly (WIRED): You practically need Google Maps directions to find the settings needed to *actually* stop Google from tracking your location. From @EmilyDreyfuss
  - Nick Short (conservative): Do you have your "location history" turned off? Doesn't matter. Google's still tracking you. [link]
  - Pascal Heyman (Belgian political figure): #Google records your location even when you tell it not to. When is Google (and others)'s massive privacy violation finally going to stop? [link to Guardian story]
  - Luke Rudkowski (conservative): Google tracks your movements, like it or not -- An Associated Press investigation found that many Google services on Android devices and iPhones store your location data even if you've used privacy settings that say they will prevent it from doing so
  - Emily Dreyfuss (WIRED): In light of the @AP's bombshell report on Google Location History, I wrote about how hard it is to find the setting to *actually* turn off your Google location tracking https://www.wired.com/story/google-location-tracking-turn-off/ …
  - Nick Confessore (NYT): How a normal user would expect to turn off Google's location tracking versus the super clear and straightforward way Google does it: [image]
  - Barton Gellman (Princeton): Respectfully note that AP, which published this important privacy story, allows advertisers and data consolidators to track your location and many other things when you visit the site. Including Google. Far from the worst news site, but still.

Google

- Reed Albergotti (The Information): The AP on Google's location tracking even when people have turned off location tracking. Shouldn't be a surprise when you're using tools created specifically for the purpose of surveillance advertising but it's still interesting.
- Ashkan Soltani (former FTC CTO): This is the confusing privacy dialogue from @google may land another @FTC inquiry. "Even with Location History paused, some Google apps automatically store time-stamped location data without asking."
- Justin Brookman (Consumer Reports, ex-FTC): *"I turned off Google Location History years ago, but just checked my phone and somehow the setting had been turned back on. □"* (Also tweeted images of help center).
- The following influential accounts have tweeted a link to associated coverage (not an exhaustive list):
  - Cory Doctorow (writer)
  - Paul Joseph Watson (Info Wars)
  - Sara Carter (Fox News)
  - Zeynep Tufecki (NYT)
  - Adam Baldwin (actor)
  - Gianni Riotta (journalist)
  - Zeke Miller (AP)
  - Josh Greenman (NY Daily News)
  - Richard Nieva (CNET)
  - Matt Drange (The Information)
  - Kevin Corke (Fox News)
  - Jonathan Lemire (AP)
  - Ryan Heath (Politico)
  - Byron Tau (WSJ)
  - Zack Whittaker (TechCrunch)
  - Justin Hendrix (NYC Media Lab)
  - Jerome Corsi (conservative writer)

Link to full social report here.

THIRD PARTY COMMENTARY:

This news cycle has drawn out negative criticisms from policy influencers, including several that are calling for an FTC investigation:

Senator Mark Warner: *"If a Google user disables location services, it is perfectly reasonable for that person to expect that apps will not continue tracking their location," Warner, the top Democrat on the Senate Intelligence Committee, said in a statement. "Unfortunately, it is frustratingly common for social media companies to have corporate practices that diverge wildly from the totally reasonable expectations of their users."* - Politico

Jonathan Mayer (former chief technologist for FCC, lead researcher for 2012 Safari issue): *"If you're going to allow users to turn off something called 'Location History,' then all the places where you maintain location history should be turned off," Mayer said. "That seems like a pretty straightforward position to have."* - Associated Press (quoted widely)

Google

Alan Butler, senior council at the Electronic Privacy Information Center: *"If Google is representing to its users that they can turn off or pause location tracking but it's nevertheless tracking their location, that seems like textbook deception to me" - WIRED*

Luther Lowe, SVP policy at Yelp: RT'd @AP's tweet

SELECT COVERAGE - UNIQUE GLOBAL:

Full list of global coverage is linked here.


TechMeme August 13, 2018.

HOME RIVER LEADERBOARDS ABOUT SPONSOR EVENTS NEWSLETTER

Top News

Ryan Nakashima / Associated Press:

Investigation finds some Google apps on Android and iPhones automatically store time-stamped location data even when the location history setting is paused – SAN FRANCISCO (AP) – Google wants to know where you go so badly that it records your movements even when you explicitly tell it not to.

Yelp: See how Google is hurting the open internet and degrading its own results Ad

More: BuzzFeed News, The Register, Wired, MacRumors, Daring Fireball, Bloomberg, CNET, BetaNews, MIT Technology Review, CNBC, Gizmodo, The Outline, Android and Me, iPhone Hacks, Mashable, TechSpot, Tom's Guide, The Mac Observer, BGR, The Hill, CBS Los Angeles, The Hacker News, Pocketables, Associated Press, Vanity Fair, KnowTechie, gHacks Technology News, Cult of Mac, Boing Boing, Slashdot, iPhone in Canada Blog, MacDailyNews, Axios, and New York Times

Tweets: @ap, @yaleprivacylab, @reedalbergotti, and @nickconfessore

TechMeme, 8/13

- Associated Press, AP Exclusive: Google tracks your movements, like it or not
- Associated Press, How to find and delete where Google knows you've been - AP News
- Axios, Google services track mobile location despite privacy settings
- Bloomberg: Google Tracks Location Data Even When Users Turn Service Off, AP Report Finds
- Boing Boing, AP and Princeton University: Google tracks location of users even when they tell it not to
- BuzzFeed, Here's How To Actually Prevent Google From Tracking Your Location
- CNET, Google is probably tracking your location, even if you turn it off, says report
- CNBC, Turning off location history doesn't stop Google from storing where you've been — here's how to limit the info it logs
- Consumer Affairs, Google stores users' location regardless of privacy settings
- Daily Mail, Google really IS recording your every move! Search firm tracks location data using your smartphone, even when you explicitly tell it not to
- Fast Company, Google tracks your movements even if you've turned location history off
- Fortune, Google Is Tracking Your Location—Even Without Your Permission, Report Says
- Gizmodo, Google Stores Location Data Even With 'Location History' Turned Off—Here's How to Stop That
- GQ, Google Reportedly Doesn't Let You Turn Off Location Tracking After All
- Mashable, Google tracks you even if you turn off 'location history': report
- Metro UK, Google is spying on where you are (even if you've disabled location tracking)
- Mic, Google is tracking your location even when you ask it to stop, study shows. Here's the fix.
- New York Post, Google tracks you even if you've asked it to stop
- PC Mag, Report: Google Tracks Location Data Even If You've Opted Out
- The Hill, Report: Google tracks users even with location history turned off

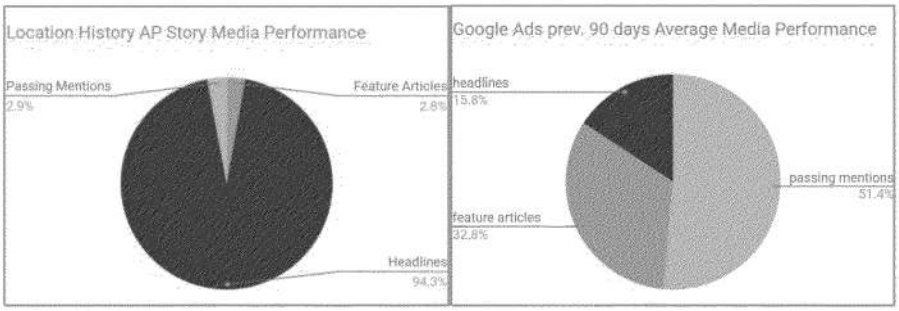
Google

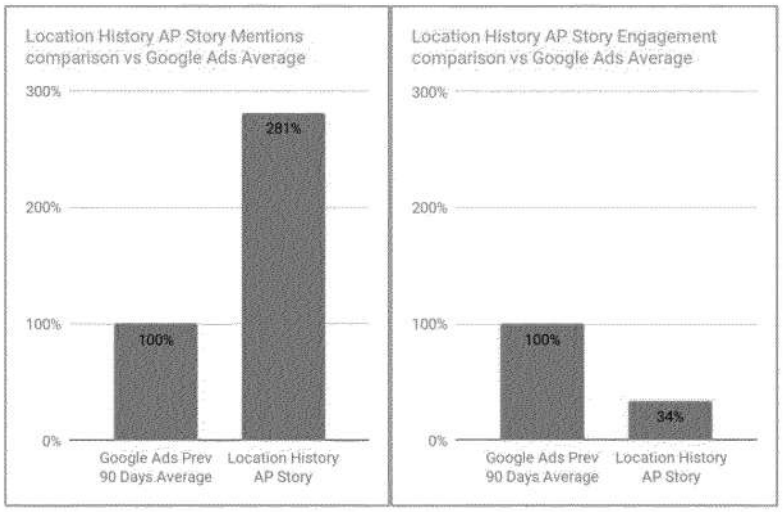
- The Sun, Google SPYING on your real-world movements even if you have Location History turned off
- The Telegraph, Google tracks your location, even when you explicitly ask it not to
- The Week, Turning off Google's location history won't stop it from tracking where you are
- Tom's Guide, Google Still Tracking Users Who Turn Off Location History
- U.S. News & World Report, Google Continuously Tracks People's Locations
- Vanity Fair, Will Google Be Washington's Next Target
- Wired, Google tracks you even if location history's off. Here's how to stop it

Shared Articles:

- Associated Press: 1,961 shares
- CTV News: 481 shares
- SBS Australia: 279 shares
- WRCB-TV Online: 200 shares
- The Hacker News: 118 shares
- NBC News: 102 shares
- MacRumors: 98 shares
- The Guardian: 91 shares
- MIT Technology Review: 70 shares
- The Real News: 62 shares
- Breitbart: 59 shares
- The Globe and Mail: 53 shares
- Common Dreams: 51 shares
- Khaleej Times: 50 shares
- The Register: 39 shares
- Fox News: 32 shares
- The Financial Express: 29 shares
- Wired: 27 shares
- CNET: 25 shares
- Gizmodo: 23 shares

Graphs:





Google

Exhibit 236

From: [redacted]
To: [redacted]
Sent: Mon, 27 Feb 2017 23:37:44 -0800
Subject: Re: [redacted]
Cc: [redacted]

[redacted]

REDACTED - PRIVILEGE

Let's say, if the users actually wanted this [redacted] which app gets what permission, [redacted] I challenge you to sketch out a solution by which device-level permissions could be enforced server-side. Remember: besides Android, we have iOS, desktop, Chrome, and a bunch of other surfaces where notions of an "app" might not even exist. Personally, I can't think of a world where we do a good and thorough job with runtime permissions across Google apps that doesn't confuse the hell out of our users and make the lives of eng and PM folk hell - by fragmenting the user base into dozens if not hundreds of odd states where the data can't flow in some directions.

I'm down to brainstorm this more with L+C and Android Platform. Like I said, Google isn't the only one 'publisher' of apps where data is shared across. Facebook and Uber are very much in the same bucket, and it's definitely broader than just location (e.g., contacts between FB main app and FB messenger seems like a very sensible data to share).

[redacted]

On Mon, Feb 27, 2017 at 6:16 PM, [redacted] wrote:

> The WAA opt-in covers gaia-keyed, long-term retention of user activity with 1st party Google products. It was originally known as the search history opt-in. In practice includes web search, maps, images, news, assistant, etc., and is used to [redacted]. It is an account-level control that is enabled by default for new accounts (except dasher). About 85% of signed-in search users have it on.

[redacted]

REDACTED - PRIVILEGE

> live independently of what is retained in location history.

On Mon, Feb 27, 2017 at 7:28 PM, [redacted] wrote:

> On Mon, Feb 27, 2017 at 3:32 PM, [redacted] wrote:

Got it, thanks [redacted]
What's WAAH opt-in? Is this a prompt that shows up during set-up? Device level or account level? One opt-in for all Google apps?

This is WAAH: [redacted]
This is [redacted] portal where all the toggles are for WAAH, LH, etc: [redacted]

I believe WAAH opt-in happens pretty liberally from a number of places, including Android setup (when Google Now is activated).
Here are a couple of slides to give you an idea of what's in WAAH and who uses it. ([redacted] correct me if only a subset of those is WAAH)

Thanks!
[redacted]

On Mon, Feb 27, 2017 at 3:20 PM, [redacted] wrote:

Thanks, [redacted]

Second scenario is not exclusive of ULR. It has to do with Web & App Activity History (aka WAAH) opt-in. A user can have both WAAH and LH - and many users do.

[redacted]
REDACTED - PRIVILEGE
[redacted]

Also, I'm fairly certain that this cross-app data sharing is it unique to Google.

Sorry, typo. I meant to say I'm fairly certain that the cross-app data sharing is NOT unique to Google.

Concrete (hypothetical, but very plausible) example: Uber and Uber Eats. Uber app has a permission to get your location. Let's say they analyze your usage and establish your daily commute routine (aka user location model). You install Uber Eats and decline it access to your location on device. Uber Eats can still determine where you are based on the user location model established from locations collected via the main Uber app.

Another example (doesn't even have to be different apps): let's say you have two devices, both running Google Now. One has location permission and one doesn't. Can Google Now give you push notifications to both devices based on locations collected on just one device?

Apps like Facebook and Uber are very likely already doing it as well, via own backends. I'm curious if Android Platform has a position on solving this more broadly.

On Mon, Feb 27, 2017 at 13:51 [redacted] wrote:

Sure, we'll follow up with [redacted], I'll include you in the review as well and you can fwd if needed (it's usually Fridays at 10am, but we have a backup [redacted] for the next few weeks, so I'll have to verify if he can attend this week).
Just so I'm clear - this use case is when the user has opted into ULR, but opted out of the app-level location permission for a Google app. That Google app could be getting location from the server through ULR/ PV/ SLF. Correct?

What's the second scenario? If the user doesn't have ULR, but is using Google App 1 and that app is saving the location points it gets and shares it in the backend with Google App 2 (who does not have app-level location permissions)? What is [redacted]

[redacted] is protobuf that encapsulates device location once it gets to a Google server. It's just a unified way to pass device location around servers. ([redacted] part of [redacted]

[redacted] is essentially where WAAH data is stored and processed.
[redacted] a backend built by Google Now team that essentially collects a bunch of signals (including current location) in both ephemeral and persistent way. I'm getting into the weeds here, so I hope [redacted] would make a drawing showing how all of these things relate to one another.

Thanks,
[redacted]

On Mon, Feb 27, 2017 at 12:16 PM, [redacted] > wrote:

On Mon, Feb 27, 2017 at 9:14 AM, [redacted] > wrote:

On Mon, Feb 27, 2017 at 8:49 AM, [redacted] > wrote:

[redacted]

> Great timing. [redacted] and I just had a conversation about location logging (in WAAH or LH) and this particular question is about location use across products (via backend channels). [redacted] is going to take a look at what products do the logging in WAAH [redacted].

My understanding is that nothing is current stopping one Google product (A) from using location logged by another Google product (B) if [redacted] approves the A<-B use. In fact, our landmark privacy policy came into existence pretty much for the very reason of enabling cross-product data use. That's why a separation on Android doesn't really make sense: Google products are currently allowed to [almost completely freely - with PWG oversight] exchange data. [redacted] do you have any thoughts on this?

> For runtime permissions, we explicitly ask the user "Allow XYZ to use location?" and the user can select Deny. I feel like we may hurt user trust if we are providing locations to XYZ via the ULR-loophole when the user has explicitly denied it. It's possible that it may not be a serious concern, but I'd be more comfortable if we have an "official policy" on this for M/N/O (in addition to planning for P/Q). Maybe discuss this in the next [redacted] meeting? [redacted], could you please add this to the agenda?

> Sounds good. To be clear - [redacted]

I don't have a very good understanding of (2) yet. [redacted] cover that area and [redacted] (cc'd) was interested in following up as well. We captured some manifestations of (2) in [redacted], so we'd like to get into next level of detail there.

I doubt that we'll find any kind of runtime permission checking on the back end; e.g., between GMM, Now, and Websearch, I'm fairly certain the location data is shared freely regardless of where it came from. I don't even think there is a technically coherent way to implement cross-app permissions outside of mobile world (how would we even do it? would the users even want it? if we had it, would it be easy to understand for anyone?).
So, it stands to reason that we should try to get the user story right on Android; Apple/iOS will probably follow (e.g., how does Uber do this?).

[redacted] would you keep us updated on what [redacted] says?
Perhaps one or two of {myself, [redacted]} could attend.

> Btw, [redacted]- do you have a sense of how permissions are enforced by Context Manager in GCore? E.g., can a 1p app (GSA/GMM/etc) get recent locations collected by ULR via Context Manager if it doesn't have direct access to device location?

[redacted]

My thinking is that we should go in the direction of [redacted]

Agreed.

[redacted]

On Mon, Feb 27, 2017 at 8:20 AM, [redacted] wrote:

> Agree the issue is not necessarily specific to [redacted]
> Do we have a list of known products not checking for permission?

On Feb 27, 2017 08:04, [redacted] > wrote:

> Hey [redacted], this [redacted] existed for 2+ years [redacted]

[redacted]

On Sun, Feb 26, 2017 at 10:19 AM, [redacted] wrote:

> In addition to solving for P/Q, we need a stopgap solution [redacted]. Can we list all the clients of [redacted], and make sure they are complying with the runtime permission?

On Fri, Feb 24, 2017 at 8:09 PM, [redacted] wrote:

> Hi [redacted] you are referring to this [redacted] right? If so, kudos to you for you being aware of it!
> It has been nagging us for ages and I'd like to see how we could structure the new Android P/Q permissions such that t[redacted]

I suggested that [redacted] - "can Google have

your Location?" - and that permission is applied, as an umbrella, to all other Google apps. There are some caveats, of course (e.g., does it apply to YouTube? Waze?), but I think this is the cleanest way to solve the problem.

[redacted] if you aren't aware of it, let's chat some more. I'd really like to solve it all together as we move forward with the new [redacted] and [redacted]

[redacted]

On Fri, Feb 24, 2017 at 4:42 PM, [redacted] > wrote:

Following our conversation, I had a question about how server-side systems (including [redacted] or [redacted]) are dealing with Android's runtime permissions.
Suppose a user has disabled permissions to, say, GMM. With client-side location, GMM will not get location, as the user intended. However, they can still get a place card (e.g. Riddler) via ULR--> [redacted] -->GMM server --> GMM client. (ULR has GmsCore's location permissions, not GMM's). This seems like a bypass to Android's permissions model.

- How are the various teams using [redacted] (e.g. Riddler) dealing with this today?
- Is there a solution other than apps "self-policing" ?

Thanks,

[redacted]

--

[redacted]

Exhibit 260

From: [redacted]
To: [redacted]
Received: Sat, 28 Jan 2017 04:27:14 +0000
Subject: Re: [redacted] for only device level settings - Invitation to edit
Cc: [redacted]

Fyi the "creates a private map" language is one of [redacted] most admired pieces of prose in the privacy space at Google. I agree.

The chrome history issue is just that if you have sWAA off you still save chrome history via sync for use in chrome, I think.

On Fri, Jan 27, 2017, 8:52 AM [redacted] wrote:

[redacted]

On Fri, Jan 27, 2017 at 6:53 AM, [redacted] wrote:

(1) The cut off line on the bottom says "Please remember that the data governed by these settings may be saved from any of your signed-in devices. You can always control and review your activity at My Account." This is just not true for the DL settings.

Which part is not true? That data (1) "may be saved from any of your signed-in devices" or that (2) "You can always control and review your activity at My Account" or both?

If it's just (1) that's wrong, it's not a big deal, because 'settings may be saved' doesn't haven't to include all the settings. If it's (2), maybe "You can control and review most of your activity at My Account"

Bear in mind, I've suggested new text for this in [redacted]. Sounds like it may need a further revision, though, based on this new information.

(1) text is accurate when the user is turning on an account-level setting. When the user is turning on a device-level setting, "these settings" only apply to that device, not all signed-in devices. (2) text is fine for account and device level settings.

(2) The language for sWAA: "Includes Chrome history and content you browse on the web in the apps". [redacted] once you mentioned that Chrome history doesn't observe sWAA. Is this right? Or did I get something wrong?

If that's true, I'm confused. Maybe I need another lesson in sWAA.

sWAA can not enable collection of Chrome History (that is controlled by Chrome Sync), but if you are a) signed in to Chrome, b) have Chrome Sync enabled, and c) have History enabled in Sync, then sWAA will include a copy of your Chrome History -- i.e., if Chrome is uploading history, then sWAA includes it in your "improve your Google experience" data bucket.

(3) Language for Location History: "Creates a private map of where you go with your signed in devices". What is should say is something along the lines of "Adds places you go with this device to your private map of where you go".

I'm not so keen on this reference to a 'private map'. The map is just the visualization. The data that is saved is the places you visit. I also think we should align on one verb for all of the settings - I think 'save' or 'store' (probably 'save') is best (we currently [redacted]

The "private map" language was a long, mostly political, fight ([redacted] is still in therapy about it). The best way to change it is to collect new user research on how alternatives test.

My preference is:

Saves where you go with this device

or

Saves places you go with this device

But I'm open to suggestions if people object.

[redacted]

On Fri, Jan 27, 2017 at 1:33 PM [redacted] wrote:

Here's what users see:



We should change language in a bunch of these.

(1) The cut off line on the bottom says "Please remember that the data governed by these settings may be saved from any of your signed-in devices. You can always control and review your activity at My Account." This is just not true for the DL settings.

(2) The language for sWAA: "Includes Chrome history and content you browse on the web in the apps". [redacted] once you mentioned that Chrome history doesn't observe sWAA. Is this right? Or did I get something wrong?

(3) Language for Location History: "Creates a private map of where you go with your signed in devices". What is should say is something along the lines of "Adds places you go with this device to your private map of where you go".

Greetings,

[redacted]

On Fri, Jan 27, 2017 at 8:19 AM [redacted] wrote:

It will look almost exactly like a sWAA and [redacted] opt-in flow, just with "for this device" / "from this device" added in some places within the text snippets.

On Thu, Jan 26, 2017, 22:32 [redacted] wrote:

I chatted w/ [redacted] about it (to see if [redacted] wanted to build their own screen) and he seemed fine with the [redacted]. Surprised me, as I thought we knew that user's don't like seeing what looks like the same scary optin multiple times.
What does the screen look like if I'm just missing device settings?

On Thu, Jan 26, 2017 at 1:20 PM, [redacted] wrote:

short answer is yes.

On Thu, Jan 26, 2017 at 1:01 PM, [redacted] (via Google Slides) [redacted] wrote:

[redacted] has invited you to **edit** the following presentation:

[redacted] for only device level settings

Hey Guys, was there ever future consideration of creating a much lighter/simpler opt-in screen when the user is only missing the device level settings?

Open in Slides

Google Slides: Create and edit presentations online.
Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
You have received this email because someone shared a presentation with you from Google Slides.

--
[redacted]

--
[redacted]
mail: [redacted]
chat: [redacted]@ Google Hangouts
visit: 1600 Amphitheater Parkway, Mountain View, CA 94043
talk [redacted]@ mobile or [redacted]@ office

--
[redacted]

--
[redacted]
mail: [redacted]
chat: [redacted] @ Google Hangouts
visit: 1600 Amphitheater Parkway, Mountain View, CA 94043
talk [redacted] @ mobile or [redacted] @ office

This page intentionally left blank for double-sided pagination and printing

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Richmond Division (The Hon. M. Hannah Lauck)

JOINT APPENDIX

VOLUME 8 of 11 (pages 1811 - 2090)

JESSICA D. ABER
United States Attorney

Kenneth R. Simon, Jr., Ass't U.S. Attorney
Peter S. Duffey, Ass't U.S. Attorney
Counsel for Appellee
919 East Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400

Nathan P. Judish, Senior Counsel
Computer Crime & Intel. Property Section
Criminal Division
U.S. Department of Justice

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
Counsel for Appellant
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800

Michael W. Price, Litigation Dir.
NACDL Fourth Amendment Ctr.
1660 L Street NW, 12th Floor
Washington, DC 20036

This page intentionally left blank for double-sided pagination and printing

TABLE OF CONTENTS

VOLUME 1 (pages 1 - 176)

District Court Docket Sheet (as of Jan. 17, 2023) 1

Indictment (Sept. 17, 2019, Doc. 1) 22

Defendant's Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Oct. 29, 2019, Doc. 29) 25

Government's Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (Nov. 19, 2019, Doc. 41) 51

Defendant's Reply to Government's Response [to] Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Dec. 9, 2019, Doc. 48) 76

Exh. A (First Step 2 Request to Google) (Doc. 48-1) 98
Exh. B (Second Step 2 Request to Google) (Doc. 48-2) 100
Exh. C (Third Step 2 Request to Google) (Doc. 48-3) 102
Exh. D (Transcript, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019)) (Doc. 48-4) ..... omitted from J.A.

Government's Notice Regarding Attachment of Google Geofence State Search Warrant to Response in Opposition to Motion to Suppress (Dec. 18, 2019, Doc. 54) 104

Affidavit for search warrant and warrant, with attachments (Doc. 54-1) 107

Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant (Dec. 20, 2019, Doc. 59-1) 118

United States' Response to Amicus Curiae Brief of Google LLC (Jan. 10, 2020, Doc. 71) 148

Defendant's Response to Google's Motion to File Amicus Curiae Brief in Support of Neither Party (Jan. 10, 2020, Doc. 72) 158

VOLUME 2 (pages 177 - 416)

Transcript, Discovery Motion Hearing (Jan. 21, 2020, Doc. 81; *see* Doc. 77 (court minutes))....177

Preliminary matters....179

Def't witness Spencer McInvaille — Direct examination....193; Cross examination....283; Redirect examination....306

Argument by the defense....318
Argument by the government....332
Rebuttal by the defense....350

Court's ruling....355

Defendant's Supplemental Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (May 22, 2020, Doc. 104)....363

United States' Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (June 12, 2020, Doc. 109)....393

VOLUME 3 (pages 417 - 694)

Transcript, Suppression Motion Hearing, Day 1 (evidence) (Mar. 4, 2021, Doc. 201; *see* Doc. 198 (court minutes))....417

Preliminary matters....420

Def't witness Spencer McInvaille — Direct examination....432; Cross examination....542; Redirect examination....586

Def't witness Marlo McGriff — Direct examination....606

VOLUME 4 (pages 695 - 1070)

Transcript, Suppression Motion Hearing, Day 2 (evidence) (Mar. 5, 2021, Doc. 202; *see* Doc. 199 (court minutes)) 695

Preliminary matters 698

Def't witness Marlo McGriff, cont'd — Direct examination ..... 699; Cross examination ..... 791; Redirect examination 841

Def't witness Sarah Rodriguez — Direct examination ..... 862; Cross examination ..... 902; Redirect examination 916

Gov't witness Jeremy D'Errico — Direct examination ..... 923; Cross examination ..... 967; Redirect examination 1010

Gov't witness Joshua Hylton — Direct examination ..... 1016; Cross examination ..... 1040; Redirect examination 1063

Concluding matters 1064

VOLUME 5 (pages 1071 - 1326)

Defendant's Post-Hearing Brief on "Geofence" General Warrant (May 3, 2021, Doc. 205) 1071

Government's Response in Opposition to Defendant's Motion for Suppression (May 21, 2020, Doc. 214; *see* Doc. 207-2) 1117

Defendant's Reply to Government's Response in Opposition to Motion for Suppression (June 4, 2020, Doc. 213) 1164

Transcript, Suppression Hearing (arguments) (June 24, 2021, Doc. 217; *see* Doc. 215 (court minutes)) 1185

Argument by the defense 1187
Argument by the government 1231
Rebuttal by the defense 1313

Concluding matters 1322

VOLUME 6 (pages 1327 - 1456)

Memorandum Opinion (denying suppression motion) (Mar. 3, 2022, Doc. 220) 1327

Order (denying suppression motion) (Mar. 3, 2022, Doc. 221) 1390

Criminal Information (May 6, 2022, Doc. 224) 1391

Transcript, Change of Plea Hearing (May 9, 2022, Doc. 247; *see* Doc. 226) 1394

Plea Agreement (May 9, 2022, Doc. 228) 1428

Statement of Facts (May 9, 2022, Doc. 229) 1444

Judgment in a Criminal Case (Aug. 19, 2022, Doc. 239) 1449

Notice of Appeal (Aug. 25, 2022, Doc. 241) 1456

VOLUME 7 (pages 1457 - 1810) – DOCUMENT EXHIBITS

Exhibits Admitted at Discovery Motion Hearing (Jan. 21, 2020)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) ..... *see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) ..... *see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) ..... *see* J.A. 2093
Def't Exh. 4: Activation Video ..... omitted from J.A., available on request
Def't Exh. 5: Three Paths Video (sealed) ..... *see* J.A. 2139
Def't Exh. 6: First Step 2 Request to Google 1457
Def't Exh. 7: Second Step 2 Request to Google 1459
Def't Exh. 8: Third Step 2 Request to Google 1461

Def't Exh. 9: Step 3 Request to Google 1463

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) .....*see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) .....*see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) .....*see* J.A. 2093
Def't Exh. 5: Three Paths Video (sealed) .....*see* J.A. 2139
Def't Exh. 6: Spencer McInvaille Report 1464
Def't Exh. 7: Spencer McInvaille Supplemental Report 1469
Def't Exh. 8: CSV Google Data File (.csv file) .....*see* J.A. 2139
Def't Exh. 9: Unique in Crowd Study 1475
Def't Exh. 11: September 2018 Oracle Submission 1480
Def't Exh. 18: Federal Search Warrant Application & Attachments 1502
Def't Exh. 19: State Search Warrants & Attachments 1534
Def't Exh. 21: McGriff Declaration 1 (Doc. 96-1) 1551
Def't Exh. 23: McGriff Declaration 3 (Doc. 147) 1562
Def't Exh. 24: Rodriguez Declaration (Doc. 96-2) 1579
Def't Exh. 27: Every Step You Take 1587
Def't Exh. 30: AZ Ex. 18 (admitted portions only) 1631
Def't Exh. 31: AZ Ex. 19 (admitted portions only) 1633
Def't Exh. 32: AZ Ex. 20 1639
Def't Exh. 33: AZ Ex. 24 1644
Def't Exh. 34: AZ Ex. 202 1667
Def't Exh. 36: AZ Ex. 209 1777
Def't Exh. 38: AZ Ex. 219 1781
Def't Exh. 40: AZ Ex. 236 1797
Def't Exh. 41: AZ Ex. 260 1804

VOLUME 8 (pages 1811 - 2090) – DOCUMENT EXHIBITS, CONT'D

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021), cont'd

Def't Exh. 43: May 2018 Privacy Policy – Redline 1811
Def't Exh. 43a: May 2018 Privacy Policy – Redline (with internet source information) 1840
Def't Exh. 44: Jan. 2019 Privacy Policy – Redline 1865
Def't Exh. 45: Oct. 2019 Privacy Policy – Redline 1895
Def't Exh. 46: McGriff Blog 1 1926

Def't Exh. 47: McGriff Blog 2 1929
Def't Exh. 48: 2018 Quartz Article 1934
Def't Exh. 49: 2018 AP Article 1 1941
Def't Exh. 51: 2019 NYT Article 1948
Def't Exh. 53: Blumenthal-Markey Letter to FTC 1957

Gov't Exh. 1: CAST PowerPoint Presentation 1981
Gov't Exh. 2: Geofence Warrant (Doc. 54-1) ..... *see* J.A. 107
Gov't Exh. 3: Declaration of Marlo McGriff (Mar. 11, 2020)
(same as Def't Exh. 21 (Doc. 96-1)) ..... *see* J.A. 1551
Gov't Exh. 3a: Declaration of Sarah Rodriguez (Mar. 11, 2020)
(same as Def't Exh. 24 (Doc. 96-2)) ..... *see* J.A. 1579
Gov't Exh. 3b: Supplemental Declaration of McGriff (June 17, 2020)
(Doc. 110-1) 2032
Gov't Exh. 3c: Third Declaration of Marlo McGriff (Aug. 7, 2020)
(same as Def't Exh. 23 (Doc. 147)) ..... *see* J.A. 1562
Gov't Exh. 4: Joshua Hylton emails with Google 2034
Gov't Exh. 5: Google Privacy Policy 2048
Gov't Exh. 5a: Google Terms of Service 2081
Gov't Exh. 6: Special Agent D'Errico's C.V. 2088
Gov't Exh. 12: "Got to Be Mobile" Video ..... *see* J.A. 2091

VOLUME 9 (pages 2091 - 2092) – DIGITAL MEDIA EXHIBIT

Gov't Exh. 12: "Got to Be Mobile" Video (admitted only at suppression motion hearing) ..... (.mp4 file)

VOLUME 10 (pages 2093 - 2138) – SEALED DOCUMENT EXHIBIT

Def't Exh. 3: PDF of Raw Data (*see* Doc. 69 (sealing order)) (admitted at both discovery motion hearing and suppression motion hearing) 2093

VOLUME 11 (pages 2139 - end) – SEALED DIGITAL MEDIA EXHIBITS

Def't Exh. 5: Three Paths Video (admitted at both discovery motion hearing and suppression motion hearing) ..... (.mp4 file)
Def't Exh. 8: CSV Google Data File (admitted only at suppression motion hearing) ..... (.csv file, viewable in Excel)

PRIVACY POLICY

Last modified: ~~December 18, 2017~~ May 25, 2018 (view archived versions)

~~There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.~~

~~Our Privacy Policy explains:~~

- ~~What information we collect and why we collect it.~~
- ~~How we use that information.~~
- ~~The choices we offer, including how to access and update information.~~

~~We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a long-time user, please do take the time to get to know our practices – and if you have any questions contact us.~~

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we

collect it, and how you can update, manage, export, and delete your information.

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for key terms. And if you have any questions about this Privacy Policy, you can contact us.

~~INFORMATION WE COLLECT~~ INFORMATION GOOGLE COLLECTS

~~We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like.~~

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll

find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

~~We collect information in the following ways:~~

Things you create or provide to us

~~**Information you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card to store with your account. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.~~

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

~~**Information we get from your use of our services.** We collect information about the~~

services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses our advertising services, or view and interact with our ads and content. This information includes:

- **Device information**

  We collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

- **Log information**

  When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes:

  - details of how you used our service, such as your search queries.
  - telephony log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
  - Internet protocol address.
  - device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
  - cookies that may uniquely identify your browser or your Google Account.

- **Location information**

  When you use Google services, we may collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that may, for example, provide Google with

information on nearby devices, Wi-Fi access points and cell towers.

- **Unique application numbers**

  Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

- **Local storage**

  We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

- **Cookies and similar technologies**

  We and our partners use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites. Our Google Analytics product helps businesses and site owners analyze the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google Analytics information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites.

Information we collect when you are signed in to Google, in addition to information we obtain about you from partners, may be associated with your Google Account. When information is associated with your Google Account, we treat it as personal information. For more information about how you can access, manage or delete information that is associated with your Google Account, visit the Transparency and choice section of this policy.

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity

- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

You can visit your Google Account to find and manage activity information that's saved in your account.

Go to Google Account

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- IP address
- Sensor data from your device
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to save and manage your location information in your account.

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

~~How we use information we collect~~ We use data to build better services

~~We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.~~

~~We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services. If other users already have your email, or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.~~

~~If you have a Google Account, we may display your Profile name, Profile photo, and actions you take on Google or on third-party applications connected to your Google Account (such as +1's, reviews you write and comments you post) in our services, including displaying in ads and other commercial contexts. We will respect the choices you make to limit sharing or visibility settings in your Google Account.~~

~~When you contact Google, we keep a record of your communication to help solve any~~

~~issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.~~

~~We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. One of the products we use to do this on our own services is Google Analytics. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. When showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health.~~

~~Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.~~

~~We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.~~

~~We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.~~

~~Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.~~

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, Security Checkup provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.

Go to Ad Settings

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

~~Transparency and choice~~

~~People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:~~

- ~~Review and update your Google activity controls to decide what types of data, such as videos you've watched on YouTube or past searches, you would like saved with your account when you use Google services. You can also visit these controls to manage whether certain activity is stored in a cookie or similar technology on your device when you use our services while signed-out of your account.~~
- ~~Review and control certain types of information tied to your Google Account by using Google Dashboard.~~
- ~~View and edit your preferences about the Google ads shown to you on Google and across the web, such as which categories might interest you, using Ads Settings. You can also visit that page to opt out of certain Google advertising services.~~
- ~~Adjust how the Profile associated with your Google Account appears to others.~~
- ~~Control who you share information with through your Google Account.~~

- ~~Take information associated with your Google Account out of many of our services.~~
- ~~Choose whether your Profile name and Profile photo appear in shared endorsements that appear in ads.~~

~~You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it's important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.~~

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the Privacy Checkup, which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our Product Privacy Guide.

Go to Privacy Checkup

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your Google Account includes:

Privacy controls

Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.

Go to Activity Controls

Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

Go to Ad Settings

About you

Control what others see about you across Google services.

Go to About You

Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

Go to Shared Endorsements

Information you share

Control whom you share information with through your account on Google+.

Go to Information You Share

Ways to review & update your information

My Activity

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

Go to My Activity

Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

Go to Dashboard

Your personal information

Manage your contact information, such as your name, email, and phone number.

Go to Personal Info

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: Choose whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your YouTube Search History and your YouTube Watch History.
- Ad Settings: Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

You can also request to remove content from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

And finally, Inactive Account Manager allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a cookie in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services rely on cookies to function properly, for things like remembering your language preferences.
- Device-level settings: Your device may have controls that determine what information we collect. For example, you can modify location settings on your Android device.

~~Information you share~~

Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google. Our services provide you with different options on sharing and removing your content.

Accessing and updating your personal information

Whenever you use our services, we aim to provide you with access to your personal information. If that information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes.

We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

Information we share

We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- **With your consent**

  We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

-

With domain administrators

If your Google Account is managed for you by a domain administrator (for example, for G Suite users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

- view statistics regarding your account, like statistics regarding applications you install.
- change your account password.
- suspend or terminate your account access.
- access or retain information stored as part of your account.
- receive your account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
- restrict your ability to delete or edit information or privacy settings.

Please refer to your domain administrator's privacy policy for more information.

-

For external processing

We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

-

For legal reasons

We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or

disclosure of the information is reasonably necessary to:

- meet any applicable law, regulation, legal process or enforceable governmental request.
- enforce applicable Terms of Service, including investigation of potential violations.
- detect, prevent, or otherwise address fraud, security or technical issues.
- protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing a song in Play, your name and photo appear next to your activity. We may also display this information in ads depending on your Shared endorsements setting.

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you use Google Home to request a ride from a ride-sharing service, we'll get your permission before sharing your address with that service. We'll ask for your explicit consent to share any sensitive personal information.

With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite), your domain administrator and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our Transparency Report.
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

~~Information security~~ We build security into our services to protect your information

~~We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular:~~

- ~~We encrypt many of our services using SSL.~~
- ~~We offer you two step verification when you access your Google Account, and a~~

~~Safe Browsing feature in Google Chrome.~~

- ~~We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.~~
- ~~We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.~~

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like Safe Browsing, Security Checkup, and 2 Step Verification to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

In some cases, we retain data for limited periods when it needs to be kept for legitimate business or legal purposes. You can read about Google's data retention periods, including how long it takes us to delete your information.

We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

European requirements

If European Union (EU) data protection law applies to the processing of your information, we provide the controls described in this policy so you can exercise your right to request access to, update, remove, and restrict the processing of your information. You also have the right to object to the processing of your information or export your information to another service.

We process your information for the purposes described in this policy, based on the following legal grounds:

With your consent

We ask for your agreement to process your information for specific purposes and you have the right to withdraw your consent at any time. For example, we ask for your consent to provide you with personalized services like ads. We also ask for your consent to collect your voice and audio activity for speech recognition. You can manage these settings in your Google Account.

When we're pursuing legitimate interests

We process your information for our legitimate interests and those of third parties while applying appropriate safeguards that protect your privacy. This means that we process your information for things like:

- Providing, maintaining, and improving our services to meet the needs of our users
- Developing new products and features that are useful for our users

- Understanding how people use our services to ensure and improve the performance of our services
- Customizing our services to provide you with a better user experience
- Marketing to inform users about our services
- Providing advertising to make many of our services freely available for users
- Detecting, preventing, or otherwise addressing fraud, abuse, security, or technical issues with our services
- Protecting against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law
- Performing research that improves our services for our users and benefits the public
- Fulfilling obligations to our partners like developers and rights holders
- Enforcing legal claims, including investigation of potential violations of applicable Terms of Service

When we're providing a service

We process your data to provide a service you've asked for under a contract. For example, we process your payment information when you buy extra storage for Google Drive.

When we're complying with legal obligations

We'll process your data when we have a legal obligation to do so, for example, if we're responding to legal process or an enforceable governmental request.

If you have questions, you can contact Google and our data protection office. And you can contact your local data protection authority if you have concerns regarding your rights under local law.

~~When this Privacy Policy applies~~ When this policy applies

~~Our Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, services Google provides on Android devices, and services offered on other sites (such as our advertising services), but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.~~

~~Our Privacy Policy does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you in search results, sites that may include Google services, or other sites linked from our services. Our Privacy Policy does not cover the information practices of other companies and organizations who advertise our services, and who may use cookies, pixel tags and other technologies to serve and offer relevant ads.~~

~~Compliance and cooperation with regulatory authorities~~

~~We regularly review our compliance with our Privacy Policy. We also adhere to several self regulatory frameworks, including the EU-US and Swiss-US Privacy Shield Frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.~~

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our

services

- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

~~Changes~~ Changes to this policy

~~Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.~~

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to archived versions for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

~~Specific product practices~~ Specific Google services

~~The following notices explain specific privacy practices with respect to certain Google products and services that you may use:~~

- ~~Chrome and Chrome OS~~
- ~~Play Books~~
- ~~Payments~~
- ~~Fiber~~
- ~~Project Fi~~

- ~~G Suite for Education~~
- ~~YouTube Kids~~
- ~~Google Accounts Managed with Family Link~~

~~For more information about some of our most popular services, you can visit the Google Product Privacy Guide.~~

The following privacy notices provide additional information about some Google services:

- Chrome & the Chrome Operating System
- Play Books
- Payments
- Fiber
- Project Fi
- G Suite for Education
- YouTube Kids
- Google Accounts Managed with Family Link

~~Other useful privacy and security related materials~~ Other useful resources

~~Further useful privacy and security related materials can be found through Google's policies and principles pages, including:~~

- ~~Information about our technologies and principles, which includes, among other things, more information on~~

- how Google uses cookies.
- technologies we use for advertising.
- how we recognize patterns like faces.

- A page that explains what data is shared with Google when you visit websites that use our advertising, analytics and social products.
- The Privacy Checkup tool, which makes it easy to review your key privacy settings.
- Google's safety center, which provides information on how to stay safe and secure online.

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- Your Google Account is home to many of the settings you can use to manage your account
- Privacy Checkup guides you through key privacy settings for your Google Account
- Google's safety center offers advice for staying safe & secure
- Google's privacy site provides more information about how we keep your information private and safe
- Privacy & Terms provides more context regarding this Privacy Policy and our Terms of Service

PRIVACY POLICY

Last modified: ~~December 18, 2017~~ May 25, 2018 (view archived versions)

~~There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.~~

~~Our Privacy Policy explains:~~

- ~~What information we collect and why we collect it.~~
- ~~How we use that information.~~
- ~~The choices we offer, including how to access and update information.~~

~~We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a long-time user, please do take the time to get to know our practices – and if you have any questions contact us.~~

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

We build a range of services that help millions of people daily to explore and interact with the

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 39 of 288Total Pages:(1905 of 2164)

world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for key terms. And if you have any questions about this Privacy Policy, you can contact us.

~~INFORMATION WE COLLECT~~ INFORMATION GOOGLE COLLECTS

~~We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like.~~

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

~~We collect information in the following ways:~~

Things you create or provide to us

Information you give us. For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card to store with your account. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

Information we get from your use of our services. We collect information about the services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses our advertising services, or view and interact with our ads and content. This information includes:

- **Device information**

  We collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

- **Log information**

  When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes:

- details of how you used our service, such as your search queries.
- telephony log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
- Internet protocol address.
- device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
- cookies that may uniquely identify your browser or your Google Account.

- **Location information**

  When you use Google services, we may collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that may, for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers.

- **Unique application numbers**

  Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

- **Local storage**

  We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

- **Cookies and similar technologies**

  We and our partners use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our

~~partners, such as advertising services or Google features that may appear on other sites. Our Google Analytics product helps businesses and site owners analyze the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google Analytics information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites.~~

~~Information we collect when you are signed in to Google, in addition to information we obtain about you from partners, may be associated with your Google Account. When information is associated with your Google Account, we treat it as personal information. For more information about how you can access, manage or delete information that is associated with your Google Account, visit the Transparency and choice section of this policy.~~

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch

- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

You can visit your Google Account to find and manage activity information that's saved in your account.

Go to Google Account

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- IP address
- Sensor data from your device
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to save and manage your location information in your account.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 44 of 288Total Pages:(1910 of 2164)

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

~~How we use information we collect~~ We use data to build better services

~~We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.~~

~~We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services. If other users already have your email, or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.~~

~~If you have a Google Account, we may display your Profile name, Profile photo, and actions you take on Google or on third-party applications connected to your Google Account (such as +1's, reviews you write and comments you post) in our services, including displaying in ads and other commercial contexts. We will respect the choices you make to limit sharing or visibility settings in your Google Account.~~

~~When you contact Google, we keep a record of your communication to help solve any issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.~~

~~We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. One of the products we use to do this on our own services is Google Analytics. For example, by saving your language preferences, we'll be able to have our services appear in the language you~~

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 45 of 288Total Pages:(1911 of 2164)

prefer. When showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health.

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.

Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first

photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, Security Checkup provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.

Go to Ad Settings

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google,

we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

~~Transparency and choice~~

~~People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:~~

- ~~Review and update your Google activity controls to decide what types of data, such as videos you've watched on YouTube or past searches, you would like saved with your account when you use Google services. You can also visit these controls to manage whether certain activity is stored in a cookie or similar technology on your device when you use our services while signed-out of your account.~~

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 48 of 288Total Pages:(1914 of 2164)

- Review and control certain types of information tied to your Google Account by using Google Dashboard.
- View and edit your preferences about the Google ads shown to you on Google and across the web, such as which categories might interest you, using Ads Settings. You can also visit that page to opt out of certain Google advertising services.
- Adjust how the Profile associated with your Google Account appears to others.
- Control who you share information with through your Google Account.
- Take information associated with your Google Account out of many of our services.
- Choose whether your Profile name and Profile photo appear in shared endorsements that appear in ads.

You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it's important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the Privacy Checkup, which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our Product Privacy Guide.

Go to Privacy Checkup

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your Google Account includes:

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 49 of 288Total Pages:(1915 of 2164)

Privacy controls

Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.

Go to Activity Controls

Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

Go to Ad Settings

About you

Control what others see about you across Google services.

Go to About You

Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

Go to Shared Endorsements

Information you share

Control whom you share information with through your account on Google+.

Go to Information You Share

Ways to review & update your information

My Activity

My Activity allows you to review and control data that's created when you use Google

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 50 of 288Total Pages:(1916 of 2164)

services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

Go to My Activity

Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

Go to Dashboard

Your personal information

Manage your contact information, such as your name, email, and phone number.

Go to Personal Info

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: Choose whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your YouTube Search History and your YouTube Watch History.
- Ad Settings: Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

You can also request to remove content from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from specific Google services

- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

And finally, Inactive Account Manager allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a cookie in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services rely on cookies to function properly, for things like remembering your language preferences.
- Device-level settings: Your device may have controls that determine what information we collect. For example, you can modify location settings on your Android device.

~~Information you share~~

~~Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google. Our services provide you with different options on sharing and removing your content.~~

~~Accessing and updating your personal information~~

~~Whenever you use our services, we aim to provide you with access to your personal information. If that information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes.~~

~~We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services,~~

we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

Information we share

We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- **With your consent**

  We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

- **With domain administrators**

  If your Google Account is managed for you by a domain administrator (for example, for G Suite users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

  - view statistics regarding your account, like statistics regarding applications you install.
  - change your account password.
  - suspend or terminate your account access.
  - access or retain information stored as part of your account.
  - receive your account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
  - restrict your ability to delete or edit information or privacy settings.

  Please refer to your domain administrator's privacy policy for more information.

-

For external processing

We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

-

For legal reasons

We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

- meet any applicable law, regulation, legal process or enforceable governmental request.
- enforce applicable Terms of Service, including investigation of potential violations.
- detect, prevent, or otherwise address fraud, security or technical issues.
- protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing a song in Play, your name and photo appear next to your

activity. We may also display this information in ads depending on your Shared endorsements setting.

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you use Google Home to request a ride from a ride-sharing service, we'll get your permission before sharing your address with that service. We'll ask for your explicit consent to share any sensitive personal information.

With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite), your domain administrator and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our Transparency Report.
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

~~Information security~~ We build security into our services to protect your information

~~We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular:~~

- ~~We encrypt many of our services using SSL.~~
- ~~We offer you two step verification when you access your Google Account, and a Safe Browsing feature in Google Chrome.~~
- ~~We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.~~
- ~~We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are~~

~~subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.~~

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like Safe Browsing, Security Checkup, and 2 Step Verification to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

In some cases, we retain data for limited periods when it needs to be kept for legitimate business or legal purposes. You can read about Google's data retention periods, including how long it takes us to delete your information.

We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

European requirements

If European Union (EU) data protection law applies to the processing of your information, we provide the controls described in this policy so you can exercise your right to request access to, update, remove, and restrict the processing of your information. You also have the right to object to the processing of your information or export your information to another service.

We process your information for the purposes described in this policy, based on the following legal grounds:

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 58 of 288Total Pages:(1924 of 2164)

With your consent

We ask for your agreement to process your information for specific purposes and you have the right to withdraw your consent at any time. For example, we ask for your consent to provide you with personalized services like ads. We also ask for your consent to collect your voice and audio activity for speech recognition. You can manage these settings in your Google Account.

When we're pursuing legitimate interests

We process your information for our legitimate interests and those of third parties while applying appropriate safeguards that protect your privacy. This means that we process your information for things like:

- Providing, maintaining, and improving our services to meet the needs of our users
- Developing new products and features that are useful for our users
- Understanding how people use our services to ensure and improve the performance of our services
- Customizing our services to provide you with a better user experience
- Marketing to inform users about our services
- Providing advertising to make many of our services freely available for users
- Detecting, preventing, or otherwise addressing fraud, abuse, security, or technical issues with our services
- Protecting against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law
- Performing research that improves our services for our users and benefits the public
- Fulfilling obligations to our partners like developers and rights holders
- Enforcing legal claims, including investigation of potential violations of applicable Terms of Service

When we're providing a service

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 59 of 288Total Pages:(1925 of 2164)

We process your data to provide a service you've asked for under a contract. For example, we process your payment information when you buy extra storage for Google Drive.

When we're complying with legal obligations

We'll process your data when we have a legal obligation to do so, for example, if we're responding to legal process or an enforceable governmental request.

If you have questions, you can contact Google and our data protection office. And you can contact your local data protection authority if you have concerns regarding your rights under local law.

~~When this Privacy Policy applies~~ When this policy applies

~~Our Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, services Google provides on Android devices, and services offered on other sites (such as our advertising services), but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.~~

~~Our Privacy Policy does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you in search results, sites that may include Google services, or other sites linked from our services. Our Privacy Policy does not cover the information practices of other companies and organizations who advertise our services, and who may use cookies, pixel tags and other technologies to serve and offer relevant ads.~~

~~Compliance and cooperation with regulatory authorities~~

~~We regularly review our compliance with our Privacy Policy. We also adhere to several self regulatory frameworks, including the EU-US and Swiss-US Privacy Shield Frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.~~

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

~~Changes~~ Changes to this policy

~~Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.~~

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to archived versions for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

~~Specific product practices~~ Specific Google services

~~The following notices explain specific privacy practices with respect to certain Google products and services that you may use:~~

- ~~Chrome and Chrome OS~~
- ~~Play Books~~
- ~~Payments~~
- ~~Fiber~~

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 61 of 288Total Pages:(1927 of 2164)

- ~~Project Fi~~
- ~~G Suite for Education~~
- ~~YouTube Kids~~
- ~~Google Accounts Managed with Family Link~~

~~For more information about some of our most popular services, you can visit the Google Product Privacy Guide.~~

The following privacy notices provide additional information about some Google services:

- Chrome & the Chrome Operating System
- Play Books
- Payments
- Fiber
- Project Fi
- G Suite for Education
- YouTube Kids
- Google Accounts Managed with Family Link

~~Other useful privacy and security related materials~~ Other useful resources

~~Further useful privacy and security related materials can be found through Google's policies and principles pages, including:~~

- ~~Information about our technologies and principles, which includes, among other things, more information on~~
  - ~~how Google uses cookies.~~
  - ~~technologies we use for advertising.~~
  - ~~how we recognize patterns like faces.~~

- ~~A page that explains what data is shared with Google when you visit websites that use our advertising, analytics and social products.~~
- ~~The Privacy Checkup tool, which makes it easy to review your key privacy settings.~~
- ~~Google's safety center, which provides information on how to stay safe and secure online.~~

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- Your Google Account is home to many of the settings you can use to manage your account
- Privacy Checkup guides you through key privacy settings for your Google Account
- Google's safety center offers advice for staying safe & secure

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

Effective ~~May 25, 2018~~January 22, 2019 | Archived versions

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for key terms. And if you have any questions about this Privacy Policy, you can contact us.

INFORMATION GOOGLE COLLECTS

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

Things you create or provide to us

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-

party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

You can visit your Google Account to find and manage activity information that's saved in your account.

Go to Google Account

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- IP address
- Sensor data from your device
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to ~~save and manage your location information in your account~~create a private map of where you go with your signed-in devices.

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including

marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

WHY GOOGLE COLLECTS DATA

We use data to build better services

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, Security Checkup provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.

Go to Ad Settings

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

YOUR PRIVACY CONTROLS

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the Privacy Checkup, which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our Product Privacy Guide.

Go to Privacy Checkup

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your Google Account includes:

Privacy controls

Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.

Go to Activity Controls

Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

Go to Ad Settings

About you

Control what others see about you across Google services.

Go to About You

Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

Go to Shared Endorsements

Information you share

Control whom you share information with through your account on Google+.

Go to Information You Share

Ways to review & update your information

My Activity

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

Go to My Activity

Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

Go to Dashboard

Your personal information

Manage your contact information, such as your name, email, and phone number.

Go to Personal Info

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: Choose whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your YouTube Search History and your YouTube Watch History.
- Ad Settings: Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

You can also request to remove content from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

And finally, Inactive Account Manager allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a cookie in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services rely on cookies to function properly, for things like remembering your language preferences.

- Device-level settings: Your device may have controls that determine what information we collect. For example, you can modify location settings on your Android device.

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing a song in Play, your name and photo appear next to your activity. We may also display this information in ads depending on your Shared endorsements setting.

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you use Google Home to ~~request a ride~~make a reservation ~~from a ride-sharing service~~through a booking service, we'll get your permission before sharing your ~~address with that service~~name or phone number with the restaurant. We'll ask for your explicit consent to share any sensitive personal information.

With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite), your domain administrator and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our Transparency Report.
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.

- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

KEEPING YOUR INFORMATION SECURE

We build security into our services to protect your information

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like Safe Browsing, Security Checkup, and 2 Step Verification to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

In some cases, we retain data for limited periods when it needs to be kept for legitimate business or legal purposes. You can read about Google's data retention periods, including how long it takes us to delete your information.

We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

ABOUT THIS POLICY

When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to archived versions for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

RELATED PRIVACY PRACTICES

Specific Google services

The following privacy notices provide additional information about some Google services:

- Chrome & the Chrome Operating System
- Play Books
- Payments
- Fiber
- ~~Project~~Google Fi
- G Suite for Education
- YouTube Kids
- Google Accounts Managed with Family Link, for Children under 13 (or applicable age in your country)

Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- Your Google Account is home to many of the settings you can use to manage your account

- Privacy Checkup guides you through key privacy settings for your Google Account
- Google's safety center ~~offers advice for staying safe & secure~~helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
- ~~Google's privacy site provides more information about how we keep your information private and safe~~
- Privacy & Terms provides more context regarding this Privacy Policy and our Terms of Service
- Technologies ~~and Principles~~ includes more information about:
    - How Google uses cookies
    - Technologies used for Advertising
    - How Google uses pattern recognition to recognize things like faces in photos
    - ~~A page that explains what data is shared with Google when you visit websites that use our advertising, analytics and social products.~~
    - How Google uses ~~data when you use our partners'~~information from sites or apps that use our services

ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." Learn more about Google ads and why you may see particular ads.

the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're

composing, Gmail will suggest addresses based on the people you contact most frequently.

phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. Learn more

payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. Learn more

devices

For example, we can use information from your devices to help you decide which device you'd like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps,

your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features.

Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. Learn more

services to make and receive calls or send and receive messages

Examples of these services include:

- Google Hangouts, for making domestic and international calls
- Google Voice, for making calls, sending text messages, and managing voicemail
- ~~Project~~Google Fi, for a phone plan

Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. Learn more

publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate.

protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account
- Photos and videos you upload to Google Photos are used to help you create albums, animations, and other creations that you can share. Learn more
- A flight confirmation email you receive may be used to create a “check-in” button that appears in your Gmail
- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it’s taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

customized search results

For example, when you’re signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can learn more here. You

may also get customized search results even when you're signed out. If you don't want this level of search customization, you can search and browse privately or turn off signed-out search personalization.

personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. Learn more

sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services.

may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. Learn more

safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against

automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.

- The “last account activity” feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. Learn more

detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

combine the information we collect

Some examples of how we combine the information we collect include:

- When you’re signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. Learn more

- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. Learn more

- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based your activity. Learn more

- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. Learn more

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

Learn more about how Google uses data when you use our partners' sites or apps.

partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. Learn more

specific Google services

For example, you can delete your blog from Blogger or a Google Site you own from Google Sites. You can also delete reviews you've left on apps, games, and other content in the Play Store.

rely on cookies to function properly

For example, we use a cookie called 'lbcs' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. Learn more

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our Transparency Report.

show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. Learn more

specific partners

For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. ~~Learn more~~Learn more about these partners and how they use your information.

servers around the world

For example, we operate data centers located around the world to help keep our products continuously available for users.

third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

appropriate safeguards

For example, we may anonymize data, or encrypt data to ensure it can't be linked to other information about you. Learn more

ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

Customizing our services

For example, we may display a Google Doodle on the Search homepage to celebrate an event specific to your country.

Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. Learn more about the companies providing business services in the EU.

Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

Cookies and similar technologies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.

Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These “server logs” typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for “cars” looks like this:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 -
740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user’s ISP. Depending on the user’s service, a different address may be assigned to the user by their service provider each time they connect to the Internet.
- `25/Mar/2003 10:15:32` is the date and time of the query.
- `http://www.google.com/search?q=cars` is the requested URL, including the search query.

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

Effective ~~January 22, 2019~~October 15 | Archived versions | Download PDF

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for key terms. And if you have any questions about this Privacy Policy, you can contact us.

INFORMATION GOOGLE COLLECTS

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

Things you create or provide to us

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-

party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

You can visit your Google Account to find and manage activity information that's saved in your account.

Go to Google Account

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- IP address
- Sensor data from your device
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our

business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

WHY GOOGLE COLLECTS DATA

We use data to build better services

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, Security Checkup provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.

Go to Ad Settings

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

YOUR PRIVACY CONTROLS

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the Privacy Checkup, which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our Product Privacy Guide.

Go to Privacy Checkup

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your Google Account includes:

Privacy controls

Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.

Go to Activity Controls

Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

Go to Ad Settings

About you

Control what others see about you across Google services.

Go to About You

Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

Go to Shared Endorsements

Information you share

~~Control~~If you're a G Suite user, control whom you share information with through your account on Google+.

Go to Information You Share

Ways to review & update your information

My Activity

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

Go to My Activity

Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

Go to Dashboard

Your personal information

Manage your contact information, such as your name, email, and phone number.

Go to Personal Info

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: Choose whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your YouTube Search History and your YouTube Watch History.
- Ad Settings: Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

You can also request to remove content from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

And finally, Inactive Account Manager allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a cookie in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services rely on cookies to function properly, for things like remembering your language preferences.

- Device-level settings: Your device may have controls that determine what information we collect. For example, you can modify location settings on your Android device.

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing ~~a song~~an app in Play, your name and photo appear next to your activity. We may also display this information in ads depending on your Shared endorsements setting.

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you use Google Home to make a reservation through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We'll ask for your explicit consent to share any sensitive personal information.

With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite),

your domain administrator and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our Transparency Report.
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

KEEPING YOUR INFORMATION SECURE

We build security into our services to protect your information

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like Safe Browsing, Security Checkup, and 2 Step Verification to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any

time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

Retaining your information

~~In some cases, we retain data for limited periods when it needs to be kept for legitimate business or legal purposes. You can read about Google's data retention periods, including how long it takes us to delete your information.~~

We retain the data we collect for different periods of time depending on what it is, how we use it, and how you configure your settings:

- Some data you can delete whenever you like, such as the content you create or upload. You can also delete activity information saved in your account, or choose to have it deleted automatically after a set period of time.
- Other data is deleted or anonymized automatically after a set period of time, such as advertising data in server logs.

- We keep some data until you delete your Google Account, such as information about how often you use our services.

- And some data we retain for longer periods of time when necessary for legitimate business or legal purposes, such as security, fraud and abuse prevention, or financial record-keeping.

When you delete data, we follow a deletion process to make sure that your data is safely and completely removed from our servers or retained only in anonymized form. We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

You can read more about Google's data retention periods, including how long it takes us to delete your information.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

ABOUT THIS POLICY

When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to archived versions for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

RELATED PRIVACY PRACTICES

Specific Google services

The following privacy notices provide additional information about some Google services:

- Chrome & the Chrome Operating System
- Play Books
- Payments

- Fiber
- Google Fi
- G Suite for Education
- YouTube Kids
- Google Accounts Managed with Family Link, for Children under 13 (or applicable age in your country)
- Voice and Audio Collection from Children's Features on the Google Assistant

Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- Your Google Account is home to many of the settings you can use to manage your account
- Privacy Checkup guides you through key privacy settings for your Google Account
- Google's safety center helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
- Privacy & Terms provides more context regarding this Privacy Policy and our Terms of Service
- Technologies includes more information about:
    - How Google uses cookies
    - Technologies used for Advertising
    - How Google uses pattern recognition to recognize things like faces in photos
    - How Google uses information from sites or apps that use our services

ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." Learn more about Google ads and why you may see particular ads.

the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you contact most frequently.

phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. Learn more

payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. Learn more

devices

For example, we can use information from your devices to help you decide which device you'd like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features.

Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. Learn more

services to make and receive calls or send and receive messages

Examples of these services include:

- Google Hangouts, for making domestic and international calls
- Google Voice, for making calls, sending text messages, and managing voicemail
- Google Fi, for a phone plan

Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. Learn more

publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate.

protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account
- Photos and videos you upload to Google Photos are used to help you create albums, animations, and other creations that you can share. Learn more
- A flight confirmation email you receive may be used to create a "check-in" button that appears in your Gmail
- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it's taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can learn more here. You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can search and browse privately or turn off signed-out search personalization.

personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. Learn more

sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services.

may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that

are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. Learn more

safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.
- The “last account activity” feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. Learn more

detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

combine the information we collect

Some examples of how we combine the information we collect include:

- When you’re signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. Learn more

- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. Learn more

- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based your activity. Learn more

- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. Learn more

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

Learn more about how Google uses data when you use our partners' sites or apps.

partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. Learn more

specific Google services

For example, you can delete your blog from Blogger or a Google Site you own from Google Sites. You can also delete reviews you've left on apps, games, and other content in the Play Store.

rely on cookies to function properly

For example, we use a cookie called 'lbcs' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. Learn more

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our Transparency Report.

show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. Learn more

specific partners

For example, we allow YouTube creators and advertisers to work with measurement

companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. Learn more about these partners and how they use your information.

servers around the world

For example, we operate data centers located around the world to help keep our products continuously available for users.

third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

appropriate safeguards

For example, we may anonymize data, or encrypt data to ensure it can't be linked to other information about you. Learn more

ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

Customizing our services

For example, we may display a Google Doodle on the Search homepage to celebrate an event specific to your country.

Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. Learn more about the companies providing business services in the EU.

Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

Cookies and similar technologies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being

sent. However, some website features or services may not function properly without cookies. Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.

Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to

such information by Google, such as information we associate with your Google Account.

Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for "cars" looks like this:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 -
740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.
- `25/Mar/2003 10:15:32` is the date and time of the query.
- `http://www.google.com/search?q=cars` is the requested URL, including the search query.
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used.
- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've visited Google, then it will

be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

SAFETY & SECURITY

Introducing auto-delete controls for your Location History and activity data

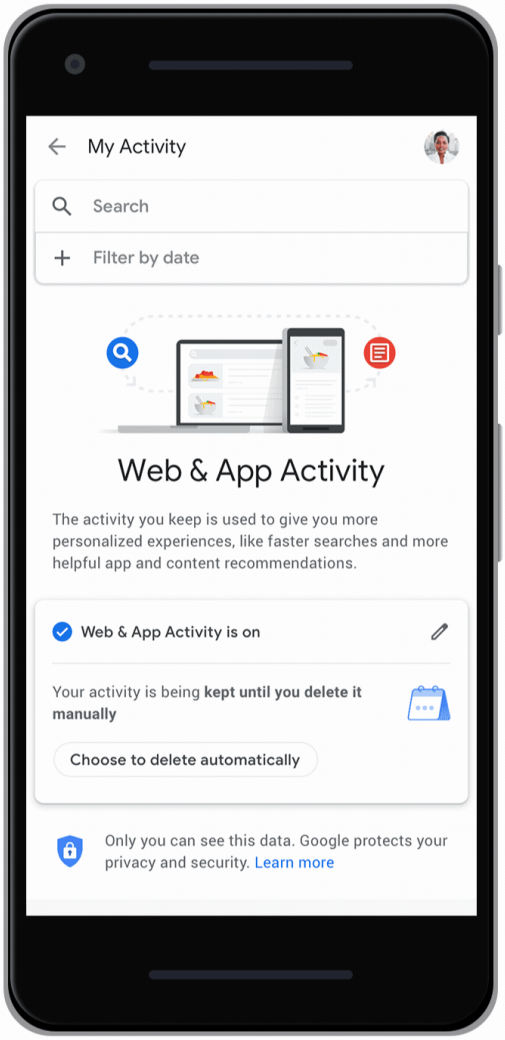
David Monsees
Product Manager, Search

Marlo McGriff
Product Manager, Maps

Published 01 May 2019

Whether you're looking for the latest news or the quickest driving route, we aim to make our products helpful for everyone. And when you turn on settings like Location History or Web & App Activity, the data can make Google products more useful for you—like recommending a restaurant that you might enjoy, or helping you pick up where you left

You can already use your Google Account to access simple on/off controls for Location History and Web & App Activity, and if you choose—to delete all or part of that data manually. In addition to these options, we're announcing auto-delete controls that make it even easier to manage your data. Here's how they'll work:



Choose a time limit for how long you want your activity data to be saved—3 or 18 months—and any data older than that will be automatically deleted from your account on an ongoing basis. These controls are coming first to Location History and Web & App Activity and will roll out in the coming weeks.

You should always be able to manage your data in a way that works best for you--and we're committed to giving you the best controls to make that happen.

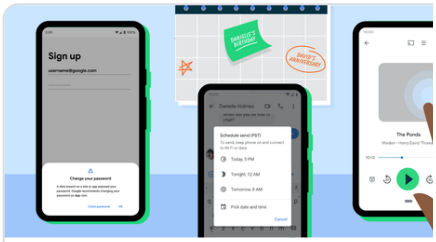
Related stories

SAFETY & SECURITY

Our efforts to fight child sexual abuse online

Our efforts to combat online child sexual exploitation and abuse, and how we're supporting organizations that are committed to protecting...

Feb 24, 2021



ANDROID

Your Android is now even safer — and 5 other new features

Feb 23, 2021

MAPS

Updates to Incognito mode and your Timeline in Maps



Marlo McGriff
Product Manager, Maps

Published 09 Dec 2019

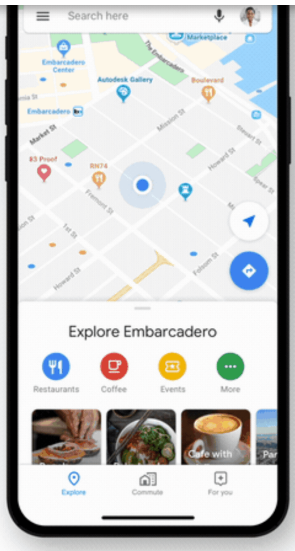
People turn to Google Maps to make their lives easier—whether it's getting tips and recommendations tailored to your daily commute, or knowing when your favorite restaurants, grocery stores and places may be the most crowded so you can avoid a long wait in line. Handy tools like this are improved by Location History–when you turn it on, this optional setting helps make Maps more useful for everyone, as well as personalized to your needs.

Throughout this year, we've focused on making it easier to control, manage and delete your Location History information. Location History is off by default, and you can choose to delete all or part of your history automatically when you turn it on. We introduced auto-delete controls so you can choose to keep only three or 18 months' worth of data—anything older than that will be automatically deleted. Your Data in Maps lets you quickly access your Location History and other privacy controls with just a few taps. And on Android, Incognito mode on Google Maps stops searches or places you navigate to within Maps from being saved to your Google Account.

Today, we have two updates: Incognito mode is rolling out on Google Maps for iOS today, and bulk delete in Timeline will arrive on Android next month.

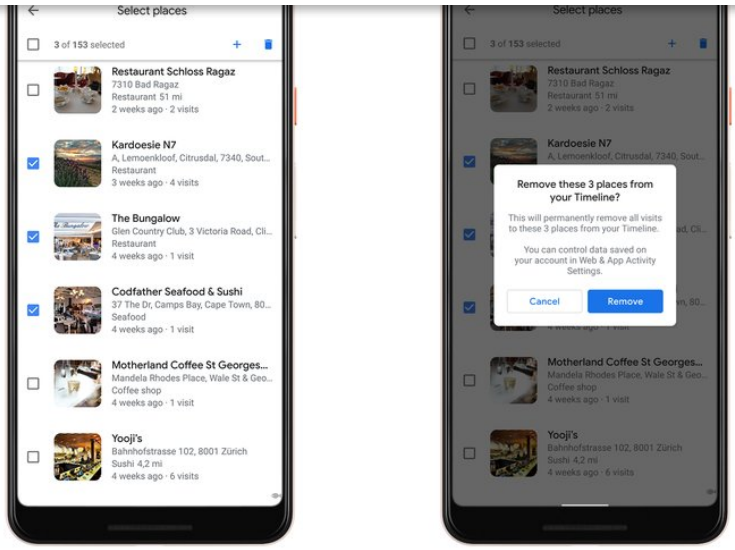
Incognito mode

Incognito mode on iOS works the same way it does on Android. While in Incognito mode, the places you search for or navigate to won't be saved to your Google Account and you won't see personalized features within Maps, like restaurant recommendations based on dining spots you've been to previously. Using Incognito mode on your phone will not update your Location History, so the places you go won't be saved to your Timeline.



Bulk delete in Timeline

Your Timeline is a tool that uses your Location History to help you easily remember places and routes you've visited–and on Android, share them with friends. With bulk delete, you can quickly find and delete multiple places from your Timeline and Location History all at once. You'll still have the ability to delete all or part of your Timeline by date range from your Location History settings.



How Location History improves Google Maps

We're committed to providing simple, easy-to-use tools to manage your Location History—as well as clearly explaining how it makes products more useful. Scroll through the images below to learn more about Google Maps features made more helpful by Location History.

Stay up to date on your Location History settings

It's our goal to help you stay informed about your Location History. If you've chosen to turn Location History on, you'll receive periodic email reminders that let you know what data you're saving, and ways you can manage it.

To learn more about Location History and how location works across Google, visit our policy page.

POSTED IN:
MAPS — SAFETY & SECURITY

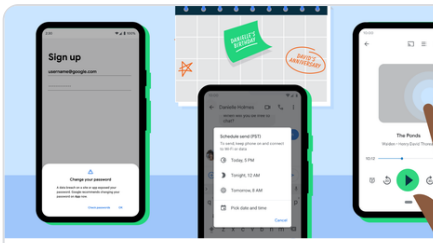
Related stories

SAFETY & SECURITY

Our efforts to fight child sexual abuse online

Our efforts to combat online child sexual exploitation and abuse, and how we're supporting organizations that are committed to protecting...

Feb 24, 2021

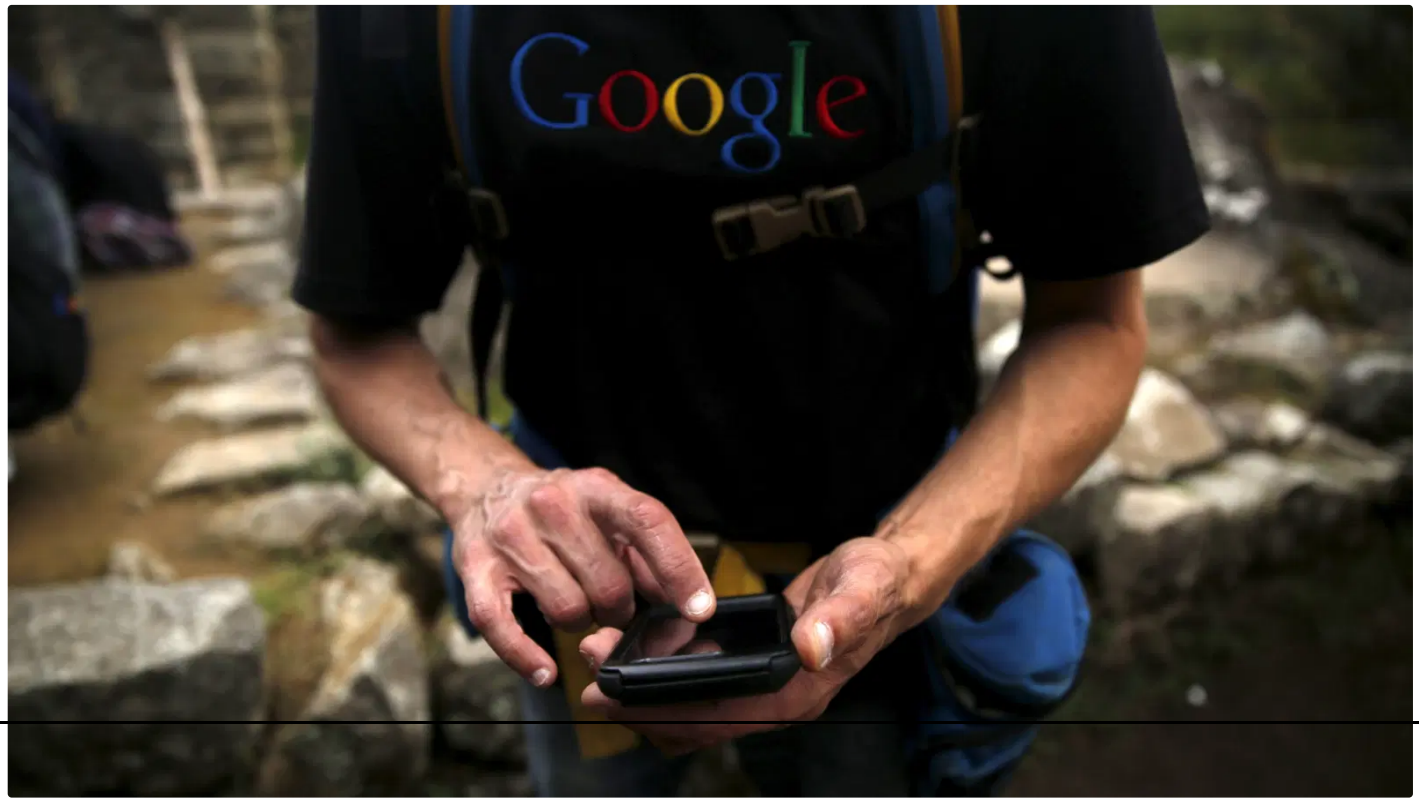


ANDROID

Your Android is now even safer — and 5 other new features

Feb 23, 2021

If you're using an Android phone, Google may be tracking every move you make



REUTERS/PILAR OLIVARES



By **David Yanofsky**
Editor of code, visuals, and data

January 24, 2018 • This article is more than 2 years old.

Biking? Google probably knows you are. Up a mountain? It probably knows that, too.

The Alphabet subsidiary's location-hungry tentacles are quietly lurking behind some of the most innovative features of its Android mobile operating system. Once those tentacles latch on, phones using Android begin silently transmitting data back to the servers of Google, including everything from GPS coordinates to nearby wifi networks, barometric pressure, and even a guess at the phone-holder's current activity. Although the product behind those transmissions is opt-in, for Android users it can be hard to avoid and even harder to understand. Opting in is also required to use several of Android's marquee features.

As a result, Google holds more extensive data on Android users than some ever realize. That data can be used by the company to sell targeted advertising. It can also be used to track into stores those consumers who saw ads on their phone or computer urging them to visit. [1] This also means governments and courts can request the detailed data on an individual's whereabouts.

While you've probably never heard of it, "Location History" is a longtime Google product with origins in the now-defunct Google Latitude. (Launched in 2009, that app allowed users to constantly broadcast their location to friends.) Today, Location History is used to power features like traffic predictions and restaurant recommendations. While it is not enabled on an Android phone by default—or even suggested to be turned on when setting up a new phone—activating Location History is subtly baked into setup for apps like Google Maps, Photos, the Google Assistant, and the primary Google app. In testing multiple phones, Quartz found that none of those apps use the same language to describe what happens when Location History is enabled, and none explicitly indicate that activation will allow every Google app, not just the one seeking permission, to access Location History data.

Quartz was able to capture transmissions of Location History information on three phones from different manufacturers, running various recent versions of Android. To accomplish this, we created a portable internet-connected wifi network that could eavesdrop and forward all of the transmissions that the devices connected to it broadcast and received. [2] None of the devices had SIM cards inserted. We walked around urban areas; shopping centers; and into stores, restaurants, and bars. The rig recorded every relevant network request [3] made by the Google Pixel 2, Samsung Galaxy S8, and Moto Z Droid that we were carrying.

According to our analysis of the phones' transmissions, this is just some of the information that gets periodically sent to Google's servers when Location History is enabled:

> A list of types of movements that your phone thinks you could be doing, by likelihood. (e.g. walking: 51%, onBicycle: 4%,

inRailVehicle: 3%)

The barometric pressure

Whether or not you're connected to wifi

The MAC address—which is a unique identifier—of the wifi access point you're connected to

The MAC address, signal strength, and frequency of every nearby wifi access point

The MAC address, identifier, type, and two measures of signal strength of every nearby Bluetooth beacon

The charge level of your phone battery and whether or not your phone is charging

The voltage of your battery

The GPS coordinates of your phone and the accuracy of those coordinates

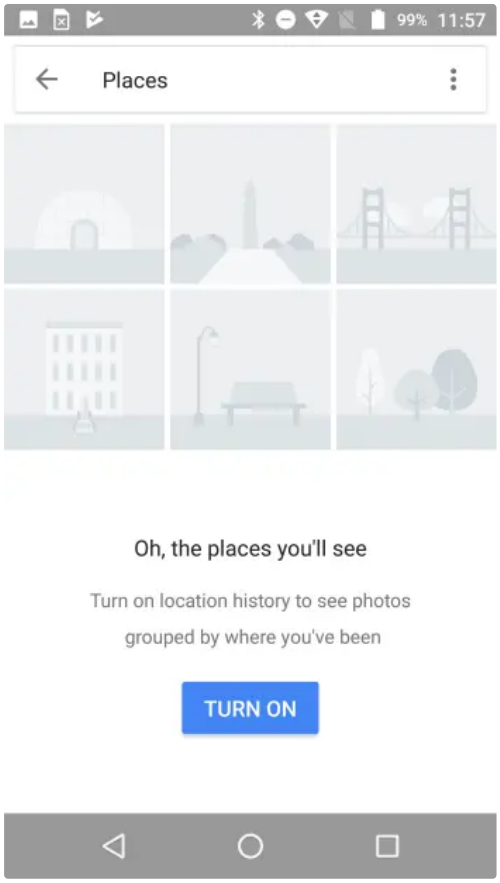
The GPS elevation and the accuracy of that

"That goes beyond what you'd expect for Location History," Bill Budington a security engineer for the Electronic Frontier Foundation, told Quartz when these transmissions were described to him, "especially in terms of predicted activity." The EFF is a nonprofit organization that advocates for digital civil liberties, freedom, and privacy, which both I and Google have made charitable contributions to in the past. [4]

Google, accurately, describes Location History as entirely opt-in. "With your permission, Google uses your Location History to deliver better results and recommendations on Google products," a spokesman wrote to Quartz in an email. "For example, you can receive traffic predictions for your daily commute, view photos grouped by locations, see recommendations based on places you've visited, and even locate a missing phone. Location History is entirely opt-in, and you can always edit, delete, or turn it off at any time."

When asked to opt in, however, the full implications of enabling Location History are rarely made clear. Here are some of the ways Google apps ask users to enable Location History.

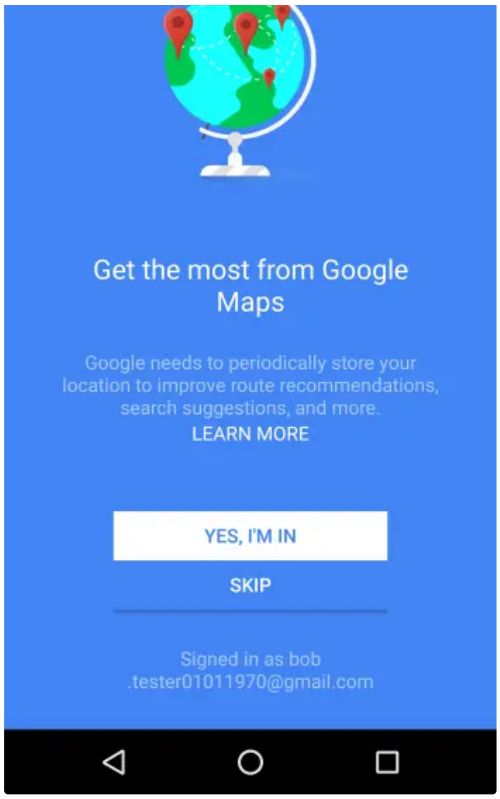
Google Photos



When the "Places" album is selected, the app requests to turn on Location History. The prompt says that Location History will allow you to "see photos grouped by where you've been." It doesn't say anything about Google using that information for other purposes. It doesn't mention that in exchange for organizing your photos, you let Google record what stores you're shopping in and what restaurants you're eating at by collecting information about nearby Bluetooth beacons and wifi networks. There is no option to limit Location History to only be used for sorting photos.

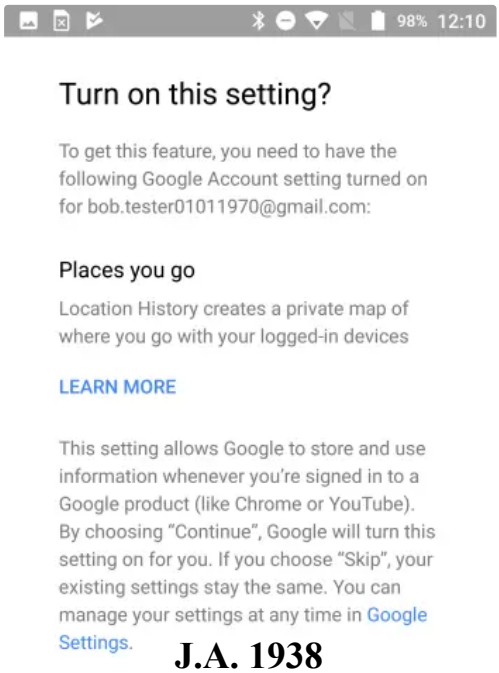
Google Maps





In Google Maps, users are encouraged to "Get the most from Google Maps" by turning on Location History. "Google needs to periodically store your location to improve route recommendations, search suggestions and more," the full-screen prompt explains. Those suggestions come in exchange for Google knowing how often you go for a run and how often you charge your battery.

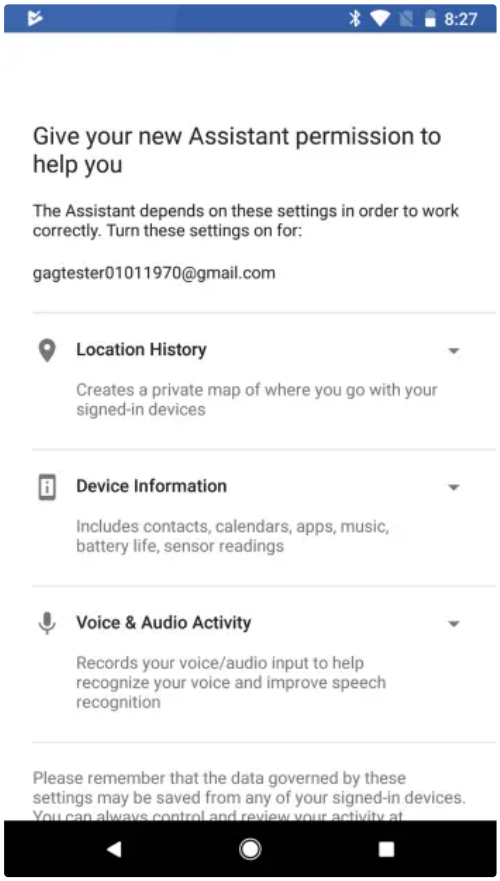
Google App





In the primary Google App, the prompt to turn on Location History occurred almost immediately on one of the Phones we tested. On another, it only appeared when trying to activate information about local road traffic. Tapping "Learn More" reveals that Google plans to use this information not just for aiding a commute, but also to give you "more useful ads on and off Google."

Google Assistant



On first use, the Google Assistant's activation screen immediately makes Location History look like a requirement. "The Assistant depends on these settings in order to work," the screen says, describing Location History as creating a "private map of where you go with your signed-in devices." [5] It makes no mention of sharing your wifi connection, only that it will "regularly obtain location data

from this device, including when you aren't using a specific Google product." Allowing these permissions is required to activate Google Assistant, although if Location History is disabled after Google Assistant is set up, the assistant will still function and does not seem to prompt for it to be re-enabled.

Google Assistant is of strategic importance to the company's efforts to keep users in its ecosystem of devices, apps, and services rather than those of Apple, Amazon, or Microsoft. Most recently, all of these companies have been focused on in-home appliances that respond to voice and can assist with various routine tasks like playing music, calling a taxi, or ordering laundry detergent.

Your Location History

Android users can check some of the information Google has collected about them by looking at "Your timeline" in Google Maps. (Google's information page on how to access it can be found here.) These instructions show how to turn off Location History entirely.

📬 **Kick off each morning with coffee and the Daily Brief (BYO coffee).**

Enter your email

By providing your email, you agree to the Quartz Privacy Policy.

apnews.com

AP Exclusive: Google tracks your movements, like it or not

By RYAN NAKASHIMA

9-11 minutes

SAN FRANCISCO (AP) — Google wants to know where you go so badly that it records your movements even when you explicitly tell it not to.

An Associated Press investigation found that many Google services on Android devices and iPhones store your location data even if you've used a privacy setting that says it will prevent Google from doing so.

Computer-science researchers at Princeton confirmed these findings at the AP's request.

For the most part, Google is upfront about asking permission to use your location information. An app like Google Maps will remind you to allow access to location if you use it for navigating. If you agree to let it record your location over time, Google Maps will display that history for you in a "timeline" that maps out your daily movements.

Storing your minute-by-minute travels carries privacy risks and has been used by police to determine the location of suspects — such as a warrant that police in Raleigh, North Carolina, served on

Google last year to find devices near a murder scene. So the company lets you "pause" a setting called Location History.

Google says that will prevent the company from remembering where you've been. Google's support page on the subject states: "You can turn off Location History at any time. With Location History off, the places you go are no longer stored."

That isn't true. Even with Location History paused, some Google apps automatically store time-stamped location data without asking. (It's possible, although laborious, to delete it .)

For example, Google stores a snapshot of where you are when you merely open its Maps app. Automatic daily weather updates on Android phones pinpoint roughly where you are. And some searches that have nothing to do with location, like "chocolate chip cookies," or "kids science kits," pinpoint your precise latitude and longitude — accurate to the square foot — and save it to your Google account.

The privacy issue affects some two billion users of devices that run Google's Android operating software and hundreds of millions of worldwide iPhone users who rely on Google for maps or search.

Storing location data in violation of a user's preferences is wrong, said Jonathan Mayer, a Princeton computer scientist and former chief technologist for the Federal Communications Commission's enforcement bureau. A researcher from Mayer's lab confirmed the AP's findings on multiple Android devices; the AP conducted its own tests on several iPhones that found the same behavior.

"If you're going to allow users to turn off something called 'Location History,' then all the places where you maintain location history should be turned off," Mayer said. "That seems like a pretty

straightforward position to have."

Google says it is being perfectly clear.

"There are a number of different ways that Google may use location to improve people's experience, including: Location History, Web and App Activity, and through device-level Location Services," a Google spokesperson said in a statement to the AP. "We provide clear descriptions of these tools, and robust controls so people can turn them on or off, and delete their histories at any time."

Google's explanation did not convince several lawmakers.

Sen. Mark Warner of Virginia told the AP it is "frustratingly common" for technology companies "to have corporate practices that diverge wildly from the totally reasonable expectations of their users," and urged policies that would give users more control of their data. Rep. Frank Pallone of New Jersey called for "comprehensive consumer privacy and data security legislation" in the wake of the AP report.

To stop Google from saving these location markers, the company says, users can turn off another setting, one that does not specifically reference location information. Called "Web and App Activity" and enabled by default, that setting stores a variety of information from Google apps and websites to your Google account.

When paused, it will prevent activity on any device from being saved to your account. But leaving "Web & App Activity" on and turning "Location History" off only prevents Google from adding your movements to the "timeline," its visualization of your daily travels. It does not stop Google's collection of other location

markers.

You can delete these location markers by hand, but it's a painstaking process since you have to select them individually, unless you want to delete all of your stored activity.

You can see the stored location markers on a page in your Google account at myactivity.google.com, although they're typically scattered under several different headers, many of which are unrelated to location.

To demonstrate how powerful these other markers can be, the AP created a visual map of the movements of Princeton postdoctoral researcher Gunes Acar, who carried an Android phone with Location history off, and shared a record of his Google account.

The map includes Acar's train commute on two trips to New York and visits to The High Line park, Chelsea Market, Hell's Kitchen, Central Park and Harlem. To protect his privacy, The AP didn't plot the most telling and frequent marker — his home address.

Huge tech companies are under increasing scrutiny over their data practices, following a series of privacy scandals at Facebook and new data-privacy rules recently adopted by the European Union. Last year, the business news site Quartz found that Google was tracking Android users by collecting the addresses of nearby cellphone towers even if all location services were off. Google changed the practice and insisted it never recorded the data anyway.

Critics say Google's insistence on tracking its users' locations stems from its drive to boost advertising revenue.

"They build advertising information out of data," said Peter Lenz,

the senior geospatial analyst at Dstillery, a rival advertising technology company. “More data for them presumably means more profit.”

The AP learned of the issue from K. Shankari, a graduate researcher at UC Berkeley who studies the commuting patterns of volunteers in order to help urban planners. She noticed that her Android phone prompted her to rate a shopping trip to Kohl’s, even though she had turned Location History off.

“So how did Google Maps know where I was?” she asked in a blog post .

The AP wasn’t able to recreate Shankari’s experience exactly. But its attempts to do so revealed Google’s tracking. The findings disturbed her.

“I am not opposed to background location tracking in principle,” she said. “It just really bothers me that it is not explicitly stated.”

Google offers a more accurate description of how Location History actually works in a place you’d only see if you turn it off — a popup that appears when you “pause” Location History on your Google account webpage . There the company notes that “some location data may be saved as part of your activity on other Google services, like Search and Maps.”

Google offers additional information in a popup that appears if you re-activate the “Web & App Activity” setting — an uncommon action for many users, since this setting is on by default. That popup states that, when active, the setting “saves the things you do on Google sites, apps, and services ... and associated information, like location.”

Warnings when you're about to turn Location History off via Android and iPhone device settings are more difficult to interpret. On Android, the popup explains that "places you go with your devices will stop being added to your Location History map." On the iPhone, it simply reads, "None of your Google apps will be able to store location data in Location History."

The iPhone text is technically true if potentially misleading. With Location History off, Google Maps and other apps store your whereabouts in a section of your account called "My Activity," not "Location History."

Since 2014, Google has let advertisers track the effectiveness of online ads at driving foot traffic , a feature that Google has said relies on user location histories.

The company is pushing further into such location-aware tracking to drive ad revenue, which rose 20 percent last year to $95.4 billion. At a Google Marketing Live summit in July, Google executives unveiled a new tool called "local campaigns" that dynamically uses ads to boost in-person store visits. It says it can measure how well a campaign drove foot traffic with data pulled from Google users' location histories.

Google also says location records stored in My Activity are used to target ads. Ad buyers can target ads to specific locations — say, a mile radius around a particular landmark — and typically have to pay more to reach this narrower audience.

While disabling "Web & App Activity" will stop Google from storing location markers, it also prevents Google from storing information generated by searches and other activity. That can limit the effectiveness of the Google Assistant, the company's digital

concierge.

Sean O'Brien, a Yale Privacy Lab researcher with whom the AP shared its findings, said it is "disingenuous" for Google to continuously record these locations even when users disable Location History. "To me, it's something people should know," he said.

___

AP Interactive: https://interactives.ap.org/google-location-tracking/

___

Associated Press writers Alan Fram and Mary Clare Jalonick in Washington and Jonathan Drew in Raleigh, North Carolina, contributed to this report.

Alex Welsh for The New York Times

Tracking Phones, Google Is a Dragnet for the Police

The tech giant records people's locations worldwide. Now, investigators are using it to find suspects and witnesses near crimes, running the risk of snaring the innocent.

By JENNIFER VALENTINO-DeVRIES APRIL 13, 2019

When detectives in a Phoenix suburb arrested a warehouse worker in a murder investigation last December, they credited a new technique with breaking open the case after other leads went cold.

The police told the suspect, Jorge Molina, they had data tracking his phone to the site where a man was shot nine months earlier. They had made the discovery after obtaining a search warrant that required Google to provide information on all devices it recorded near the killing, potentially capturing the whereabouts of anyone in the area.

Investigators also had other circumstantial evidence, including security video of someone firing a gun from a white Honda Civic, the same model

that Mr. Molina owned, though they could not see the license plate or attacker.

But after he spent nearly a week in jail, the case against Mr. Molina fell apart as investigators learned new information and released him. Last month, the police arrested another man: his mother's ex-boyfriend, who had sometimes used Mr. Molina's car.

The warrants, which draw on an enormous Google database employees call Sensorvault, turn the business of tracking cellphone users' locations into a digital dragnet for law enforcement. In an era of ubiquitous data gathering by tech companies, it is just the latest example of how personal information — where you go, who your friends are, what you read, eat and watch, and when you do it — is being used for purposes many people never expected. As privacy concerns have mounted among consumers, policymakers and regulators, tech companies have come under intensifying scrutiny over their data collection practices.

The Arizona case demonstrates the promise and perils of the new investigative technique, whose use has risen sharply in the past six months, according to Google employees familiar with the requests. It can help solve crimes. But it can also snare innocent people.

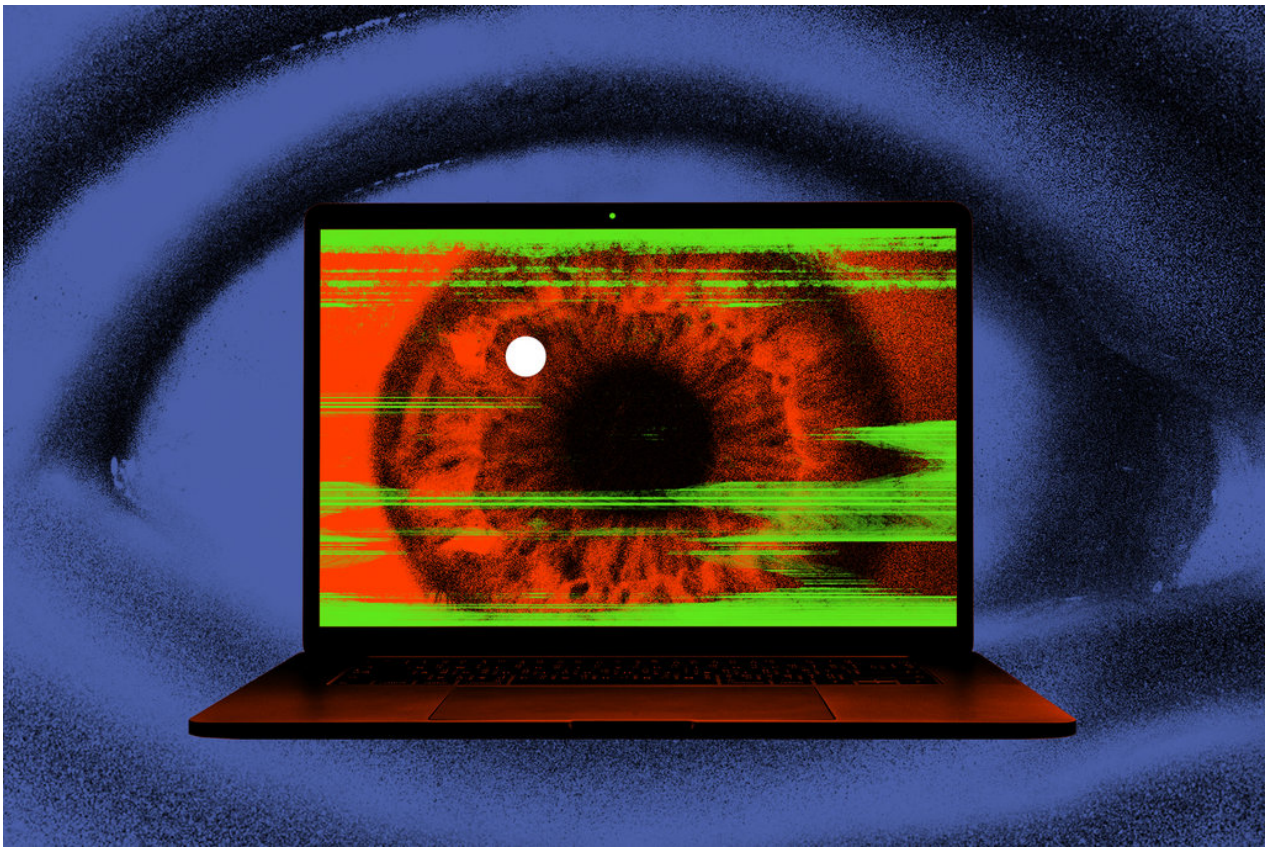
Technology companies have for years responded to court orders for specific users' information. The new warrants go further, suggesting possible suspects and witnesses in the absence of other clues. Often, Google employees said, the company responds to a single warrant with location information on dozens or hundreds of devices.

Law enforcement officials described the method as exciting, but cautioned that it was just one tool.

Opinion

The Privacy Project

The New York Times is launching an ongoing examination of privacy. We'll dig into the ideas, history and future of how our information navigates the digital ecosystem and what's at stake.



"It doesn't pop out the answer like a ticker tape, saying this guy's guilty," said Gary Ernsdorff, a senior prosecutor in Washington State who has worked on several cases involving these warrants. Potential suspects must still be fully investigated, he added. "We're not going to charge anybody just because Google said they were there."

It is unclear how often these search requests have led to arrests or convictions, because many of the investigations are still open and judges frequently seal the warrants. The practice was first used by federal agents in 2016, according to Google employees, and first publicly reported last year in North Carolina. It has since spread to local departments across the country, including in California, Florida, Minnesota and Washington. This year, one Google employee said, the company received as many as 180 requests in one week. Google declined to confirm precise numbers.

The technique illustrates a phenomenon privacy advocates have long referred to as the "if you build it, they will come" principle — anytime a technology company creates a system that could be used in surveillance, law enforcement inevitably comes knocking. Sensorvault, according to Google employees, includes detailed location records involving at least hundreds of millions of devices worldwide and dating back nearly a decade.

The new orders, sometimes called “geofence” warrants, specify an area and a time period, and Google gathers information from Sensorvault about the devices that were there. It labels them with anonymous ID numbers, and detectives look at locations and movement patterns to see if any appear relevant to the crime. Once they narrow the field to a few devices they think belong to suspects or witnesses, Google reveals the users’ names and other information.

“There are privacy concerns that we all have with our phones being tracked — and when those kinds of issues are relevant in a criminal case, that should give everybody serious pause,” said Catherine Turner, a Minnesota defense lawyer who is handling a case involving the technique.

Investigators who spoke with The New York Times said they had not sent geofence warrants to companies other than Google, and Apple said it did not have the ability to perform those searches. Google would not provide details on Sensorvault, but Aaron Edens, an intelligence analyst with the sheriff’s office in San Mateo County, Calif., who has examined data from hundreds of phones, said most Android devices and some iPhones he had seen had this data available from Google.

In a statement, Richard Salgado, Google’s director of law enforcement and information security, said that the company tried to “vigorously protect the privacy of our users while supporting the important work of law enforcement.” He added that it handed over identifying information only “where legally required.”

Mr. Molina, 24, said he was shocked when the police told him they suspected him of murder, and he was surprised at their ability to arrest him based largely on data.

“I just kept thinking, You’re innocent, so you’re going to get out,” he said, but he added that he worried that it could take months or years to be exonerated. “I was scared,” he said.

A Novel Approach

Detectives have used the warrants for help with robberies, sexual assaults, arsons and murders. Last year, federal agents requested the data to investigate a string of bombings around Austin, Tex.

Austin investigators obtained another warrant after a fourth bomb exploded. But the suspect killed himself three days after that bomb, as they were closing in. Officials at the time said surveillance video and receipts for suspicious purchases helped identify him.

An F.B.I. spokeswoman declined to comment on whether the response from Google was helpful or timely, saying that any question about the technique "touches on areas we don't discuss."

Officers who have used the warrants said they showed promise in finding suspects as well as witnesses who may have been near the crime without realizing it. The searches may also be valuable in cold cases. A warrant last year in Florida, for example, sought information on a murder from 2016. A Florida Department of Law Enforcement spokeswoman declined to comment on whether the data was helpful.

The approach has yielded useful information even if it wasn't what broke the case open, investigators said. In a home invasion in Minnesota, for example, Google data showed a phone taking the path of the likely intruder, according to a news report and police documents. But detectives also cited other leads, including a confidential informant, in developing suspects. Four people were charged in federal court.

According to several current and former Google employees, the Sensorvault database was not designed for the needs of law enforcement, raising questions about its accuracy in some situations.

Though Google's data cache is enormous, it doesn't sweep up every phone, said Mr. Edens, the California intelligence analyst. And even if a location is recorded every few minutes, that may not coincide with a shooting or an assault.

Google often doesn't provide information right away, investigators said. The Google unit handling the requests has struggled to keep up, so it can take weeks or months for a response. In the Arizona investigation, police received data six months after sending the warrant. In a different Minnesota case this fall, it came in four weeks.

But despite the drawbacks, detectives noted how precise the data was and how it was collected even when people weren't making calls or using apps — both improvements over tracking that relies on cell towers.

"It shows the whole pattern of life," said Mark Bruley, the deputy police chief in Brooklyn Park, Minn., where investigators have been using the technique since this fall. "That's the game changer for law enforcement."

A Trove of Data

Location data is a lucrative business — and Google is by far the biggest player, propelled largely by its Android phones. It uses the data to power advertising tailored to a person's location, part of a more than $20 billion market for location-based ads last year.

In 2009, the company introduced Location History, a feature for users who wanted to see where they had been. Sensorvault stores information on anyone who has opted in, allowing regular collection of data from GPS signals, cellphone towers, nearby Wi-Fi devices and Bluetooth beacons.

People who turn on the feature can see a timeline of their activity and get recommendations based on it. Google apps prompt users to enable Location History for things like traffic alerts. Information in the database is held indefinitely, unless the user deletes it.

"We citizens are giving this stuff away," said Mr. Ernsdorff, the Washington State prosecutor, adding that if companies were collecting data, law enforcement should be able to obtain a court order to use it.

Current and former Google employees said they were surprised by the warrants. Brian McClendon, who led the development of Google Maps and related products until 2015, said he and other engineers had assumed the police would seek data only on specific people. The new technique, he said, "seems like a fishing expedition."

Uncharted Legal Territory

The practice raises novel legal issues, according to Orin Kerr, a law professor at the University of Southern California and an expert on criminal law in the digital age.

One concern: the privacy of innocent people scooped up in these searches. Several law enforcement officials said the information remained sealed in their jurisdictions but not in every state.

In Minnesota, for example, the name of an innocent man was released to a local journalist after it became part of the police record. Investigators had his information because he was within 170 feet of a burglary. Reached by a reporter, the man said he was surprised about the release of his data and thought he might have appeared because he was a cabdriver. “I drive everywhere,” he said.

These searches also raise constitutional questions. The Fourth Amendment says a warrant must request a limited search and establish probable cause that evidence related to a crime will be found.

Warrants reviewed by The Times frequently established probable cause by explaining that most Americans owned cellphones and that Google held location data on many of these phones. The areas they targeted ranged from single buildings to multiple blocks, and most sought data over a few hours. In the Austin case, warrants covered several dozen houses around each bombing location, for times ranging from 12 hours to a week. It wasn’t clear whether Google responded to all the requests, and multiple officials said they had seen the company push back on broad searches.

Last year, the Supreme Court ruled that a warrant was required for historical data about a person’s cellphone location over weeks, but the court has not ruled on anything like geofence searches, including a technique that pulls information on all phones registered to a cell tower.

Google’s legal staff decided even before the 2018 ruling that the company would require warrants for location inquiries, and it crafted the procedure that first reveals only anonymous data.

“Normally we think of the judiciary as being the overseer, but as the technology has gotten more complex, courts have had a harder and harder time playing that role,” said Jennifer Granick, surveillance and cybersecurity counsel at the American Civil Liberties Union. “We’re depending on companies to be the intermediary between people and the government.”

In several cases reviewed by The Times, a judge approved the entire procedure in a single warrant, relying on investigators’ assurances that they

would seek data for only the most relevant devices. Google responds to those orders, but Mr. Kerr said it was unclear whether multistep warrants should pass legal muster.

Some jurisdictions require investigators to return to a judge and obtain a second warrant before getting identifying information. With another warrant, investigators can obtain more extensive data, including months of location patterns and even emails.

Mixed Results

Investigators in Arizona have never publicly disclosed a likely motive in the killing of Joseph Knight, the crime for which Mr. Molina was arrested. In a court document, they described Mr. Knight, a 29-year-old aircraft repair company employee, as having no known history of drug use or gang activity.

Detectives sent the geofence warrant to Google soon after the murder and received data from four devices months later. One device, a phone Google said was linked to Mr. Molina's account, appeared to follow the path of the gunman's car as seen on video. His carrier also said the phone was associated with a tower in roughly the same area, and his Google history showed a search about local shootings the day after the attack.

After his arrest, Mr. Molina told officers that Marcos Gaeta, his mother's ex-boyfriend, had sometimes taken his car. The Times found a traffic ticket showing that Mr. Gaeta, 38, had driven that car without a license. Mr. Gaeta also had a lengthy criminal record.

While Mr. Molina was in jail, a friend told his public defender, Jack Litwak, that she was with him at his home about the time of the shooting, and she and others provided texts and Uber receipts to bolster his case. His home, where he lives with his mother and three siblings, is about two miles from the murder scene.

Mr. Litwak said his investigation found that Mr. Molina had sometimes signed in to other people's phones to check his Google account. That could lead someone to appear in two places at once, though it was not clear whether that happened in this case.

Mr. Gaeta was arrested in California on an Arizona warrant. He was then charged in a separate California homicide from 2016. Officials said that case would probably delay his extradition to Arizona.

A police spokesman said “new information came to light” after Mr. Molina’s arrest, but the department would not comment further.

Months after his release, Mr. Molina was having trouble getting back on his feet. After being arrested at work, a Macy’s warehouse, he lost his job. His car was impounded for investigation and then repossessed.

The investigators “had good intentions” in using the technique, Mr. Litwak said. But, he added, “they’re hyping it up to be this new DNA type of forensic evidence, and it’s just not.”

Michael LaForgia contributed reporting. Kitty Bennett contributed research.

Related Coverage

- Google’s Sensorvault Is a Boon for Law Enforcement. This Is How It Works. APRIL 13, 2019
- Hundreds of Apps Can Empower Stalkers to Track Their Victims MAY 19, 2018
- Service Meant to Monitor Inmates’ Calls Could Track You, Too MAY 10, 2018

© 2021 The New York Times Company

United States Senate
WASHINGTON, DC 20510

May 11, 2018

The Honorable Joseph Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairman Simons:

We write to bring to your attention our concerns regarding Google's collection of sensitive location data within its "Location History" service, and to urge you to investigate any deceptive acts and practices associated with the product. As recent events have demonstrated, the American public is increasingly concerned about the stockpiling of intimate data on their personal lives unknowingly collected from their online accounts and devices. Based on our investigation and public reports on Location History, we have significant reservations about Google's failure to clearly account for how that location data is collected and used by the company.

Since 2009, Google has promoted continuous tracking of user location within several of its products through a service now called Location History. When a user enables Location History, they not only provide Google with periodic data from one device, they deepen the volume and invasiveness of collection across devices and on a continuous basis. While Google describes the tracking as an opt-in feature, our own investigation found that the consent process frequently mischaracterizes the service and degrades the functionality of products in order to push users into providing permission. This conflicts with recent industry-wide changes to improve privacy on smartphones, particularly where Google forces users on Apple devices to enable more permissive settings. Moreover, Google does not offer full and accessible information to consumers on the use of their data, including in advertising and commercial analytics services. These factors raise serious questions about whether users are able to provide informed consent.

Based on our longstanding concerns regarding digital tracking, we wrote to Google demanding a full explanation of their collection of location data on December 1, 2017 (Attachment 1). Google replied in a letter dated January 12, 2018 (Attachment 2).

There has been a long established, bipartisan recognition that precise geolocation data is sensitive—raising expectations of user consent and notification. This means there should be clear opt-in consent to collect this information. Yet, Google's policies, documentation, and response

letter raise questions about their characterization of basic consumer protection terms such as "opt-in", "opt-out", "notice", "consent", and "anonymization." Google claims Google Location History is opt-in, but both the device and application settings on Android phones frequently pushes users into providing "consent." Often the actual user choice is a screen that provides two choices, neither of which is a clear "No" (see Attachment 3). This set of options is inadequate and the confusing consent process is replicated throughout Android's various settings, where location privacy is often mischaracterized or subdivided so few users could effectuate their choice to opt-out of Google's location data gathering (see Attachment 4).

In January, *Quartz* published a detailed article on the service and Google's failure to provide an effective opt out of collection.[1] *Quartz*'s technical investigation found that when Location History is enabled, Google reported back even more device sensor information than usual, including barometric pressure, wireless signal information, battery status, and a determination about how the user is moving (such as whether they are on a bicycle). In its response letter, Google acknowledged that when Location History is on, it stores additional information from publicly-available Bluetooth "beacons," low-power devices intended to provide proximity experiences to businesses.[2] These sensors provide Google with not simply an understanding of what city a user is currently in, but the exact floor and movements within a building.

Once a user allows Location History in one application, they enter into the expansive and continuous collection of location data that is not adequately communicated to users. Google describes Location History as an 'account-level setting,' which means that Google defaults to collection across all devices that a user is logged into. This data is collected from users even when an individual is not actively using a Google application.[3] On Apple's iOS devices, Google forces users to downgrade privacy settings that would otherwise only allow tracking when an app is open in order to use features that require Location History – effectively, users have to allow Google to always track them or not use the features at all. Since Google does not provide periodic reminders or clear indication that Location History is on, users can easily enable the service and have their location monitored well beyond their intended use of the application.

Our concerns regarding Google's push for location tracking are exacerbated by the company's opacity regarding the use of this data. Consumers have a right to know how their sensitive information is used, particularly when it comes to commercial purposes. Google typically describes Location History as a service to provide "better results and recommendations

---

[1] Yanofsky , David. "If You're Using an Android Phone, Google May Be Tracking Every Move You Make." Quartz. January 24, 2018. https://qz.com/1183559/if-youre-using-an-android-phone-google-may-be-tracking-every-move-you-make/.

[2] Letter from Molinari, Susan (Google). Received by Senators Blumenthal and Markey, 12 Jan. 2018: "There are other Google products that may scan and collect certain information from Bluetooth beacons near the device. This includes information that any Bluetooth beacon may be publicly broadcasting for use, such as beacon type, beacon identifier, signal strength, and broadcast power. For example, if a user has turned on the opt-in Location History feature for their Google account, Google will use publicly available beacon information as one signal to help determine location."

[3] "When you turn on Location History, Google remembers your location on all devices where you're signed in, even when you're not using the app." from "View or Edit Your Timeline." Google Maps Help. https://support.google.com/maps/answer/6258979?co=GENIE.Platform%3DAndroid&hl=en.

on Google products," offering an example of recommending new places or giving traffic predictions. Google does not provide a full and explicit account of its use of the Location History in products and services, only including mentions of improving "location accuracy" and "battery life."[4] Further information is often only found in passing reference across disparate and unrelated product information pages intended for different audiences.

For example, in its "Business Help" page, Google states that Location History is used to provide information for businesses on Maps and Search related to popular times, wait times, and visit duration.[5] This disclosure is not offered to consumers. Google makes no mention of the use of Location History for advertising purposes in its consent mechanisms, despite the fact that it clearly uses this data for ad targeting and analytics. A general purpose "Why you may see particular ads" page states that Google uses location information in ad products to infer demographic information. While that page does not disclose how it infers location, another help page includes an example scenario that indicates Location History data is used in targeting of advertisements:[6]

> *Dorothy gives her mailing address to an online athletics store when she buys a pair of sneakers. This athletics store puts Dorothy's mailing address in its customer database, then shares its list of mailing addresses with Google. Google matches this list with addresses associated with Google accounts (ex: addresses saved in Google Maps, or* ***addresses from location history*** *[emphasis added]). Later, when Dorothy is signed in to Google and is browsing online, she may see an ad from the athletics store.*

This example describes the AdWords Customer Match service that allows advertisers to upload their list of customers to continue to target them as they browse the Internet.[7]

While many of the practices described implicates further consumer protection and privacy concerns, the troubling potential of this tracking is exemplified within the description of Google's "store visits" advertisement service:[8]

> *Store visits are measured exclusively using data from Google users who have activated Location History, which provides a location timeline, stored against the user's Google Account. Google correlates the observed store visits from those users who have activated Location History with those users' ad clicks and then uses that data to estimate the aggregate number of store visits for all users who clicked on the advertiser's ads.*

In December 2014, Google announced Store Visits analytics to provide aggregated reports of visits to retail locations by Google users who had clicked on an ad for the advertiser's

---

[4] "Manage or Delete Your Location History." Google Account Help. https://support.google.com/accounts/answer/3118687?hl=en.
[5] "Popular Times, Wait Times, and Visit Duration." Google My Business Help. https://support.google.com/business/answer/6263531?hl=en.
[6] "Why You're Seeing an Ad." Google Ads Help. https://support.google.com/ads/answer/7029660?hl=en.
[7] "About Customer Match." Google AdWords Help. https://support.google.com/adwords/answer/6379332?hl=en.
[8] Letter from Molinari, Susan (Google).

products or services.[9] Google has expanded its use of Location History in advertising analytics since its introduction. In March 2017, Google announced that it had applied "deep learning models" to provide better accuracy for multi-story malls and dense geographies.[10] Last October, Google announced that it will provide "impression-based store visits." With the change, Google will provide advertisers with information on whether people visit stores just based on seeing the advertisement, even if they do not click it.[11]

Google has also expanded the amount of information provided to advertisers, including the time taken for people to visit a store after clicking an ad, how many store visits come from repeat customers, and demographics on which groups are more likely to visit the store. In fact, Google's response revealed, "Google uses location information in our ads products to infer **demographic information** [emphasis added], to improve the relevance of the ads users see, to measure ad performance, and to report aggregate statistics to advertisers." We are particularly concerned about the use of location data for demographic inferences.

The power of this fine-grain, large-scale monitoring of the behaviors and movements of consumers is illustrated within Google's regular blog posts about holiday shopping habits provided by the Location History data.[12] Google has an intimate understanding of personal lives as they watch their user's seek the support of reproductive health services, engage in civic activities, or attend places of religious worship. All that it takes for users to expose themselves to this collection is to once allow an ambiguously described feature, for example when trying to display photos on a map on the Google Photo service, silently enabling the feature across devices with no expiration date. A feature that is only intended by a user to add city information to pictures is then opaquely used to precisely track people into stores for advertisers. Products like Store Visits and Customer Match bridge people's online activities with their daily lives in ways that they are not fully informed of.

Most consumers do not understand the level, granularity, and reach of Google's data collection, and there are serious questions about whether they have provided their informed consent and maintain a reasonable ability to avoid participating in this collection.

We are strong supporters of the FTC and its consumer protection mission. We have long advocated for robust enforcement where consumer harm is present. Congress empowered the FTC with a broad consumer enforcement mandate because it wanted the FTC to evolve with the marketplace. Today, data privacy and cybersecurity are two of the most important issues for consumers, and the loss of control over their personal data could have serious consequences for our economy.

---

[9] "Measure More: Improving Estimated Total Conversions with Store Visit Insights." Google Inside AdWords. December 18, 2014. https://adwords.googleblog.com/2014/12/measure-more-improving-estimated-total.html.
[10] "New Measurement Innovations Unlock More Store Visits Data." Google Inside AdWords. March 29, 2017. https://adwords.googleblog.com/2017/03/new-measurement-innovations-unlock-more.html.
[11] "Unwrapping New Innovations for the Holidays and Beyond." Google Inside AdWords. October 24, 2017. https://adwords.googleblog.com/2017/10/unwrapping-new-innovations-for-holidays.html.
[12] "How Consumers Will Shop—and What They'll Buy—This Holiday Season." Google Inside AdWords. November 22, 2016. https://adwords.googleblog.com/2016/11/how-consumers-will-shopand-what-theyll.html.

We ask that you review Google's response, our attachments, and their privacy policies and open an investigation into the potential deceptive acts and practices used by Google to track and commoditize American consumers.

Sincerely,

RICHARD BLUMENTHAL
United States Senator

EDWARD J. MARKEY
United States Senator

Attachment 1

Letter from Senators Blumenthal and Markey, 1 Dec. 2018

RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES:

AGING

ARMED SERVICES

COMMERCE, SCIENCE, AND TRANSPORTATION

JUDICIARY

VETERANS' AFFAIRS

United States Senate

WASHINGTON, DC 20510

706 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
FAX: (202) 224-9673

90 STATE HOUSE SQUARE, TENTH FLOOR
HARTFORD, CT 06103
(860) 258-6940
FAX: (860) 258-6958

915 LAFAYETTE BOULEVARD, SUITE 304
BRIDGEPORT, CT 06604
(203) 330-0598
FAX: (203) 330-0608

http://blumenthal.senate.gov

December 1, 2017

Mr. Sundar Pichai
CEO
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai:

According to a concerning new investigation by the publication *Quartz*, Android devices are continually and covertly collecting users' location information and sending this information to Google – even when location services are disabled, the phone has been reset to factory condition, no apps are running or the SIM card is removed.[1] These practices, which Google confirmed in the article, are alarming, and the public deserves a full explanation from the company's CEO of the reason behind this data collection.

To date, Google's explanation for this location tracking behavior has been inadequate. As you know, the Federal Trade Commission has long considered it necessary to get affirmative opt-in consent before gathering consumer geolocation data due to the sensitive nature of that data. Furthermore, I am concerned you have not been candid with why this intrusive user tracking mechanism was implemented and to what extent Google is actually committed to ceasing collection of user location data.

As the Ranking Member of the Senate Commerce Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, a member of the Senate Judiciary Committee, and longtime advocate for consumer privacy protections, I respectfully request responses on the following questions:

1) Google's privacy policy asserts, "When you use Google services, we *may* [emphasis added] collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that *may* [emphasis added], for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers." Under what circumstances "may" Google collect this data? Under what circumstances does Google *always* collect this data? Under what circumstances does Google *never* collect this data? What do you mean by "when you use Google services?" Is *all* of Android's operating system a Google service? What do you specifically mean by "nearby devices?"

[1] Collins, Keith. Google collects Android users' locations even when location services are disabled." *Quartz*, 21 Nov. 2017. qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/ .

2) If a user goes "offline" and disconnects their mobile phone from the Internet for a period of time, or even places the device in so-called "airplane mode," does Google receive location data, Wi-Fi data, cell tower data, during this "offline" time period, even if location services is still on?

3) What location data does Google specifically collect from Android users and under what circumstances? Is the location data associated with a specific device ID? Is it associated with a specific user ID? Are there any other specific user or device identifiers involved? Can you please attach to your response examples of any relevant files or server logs transmitted by an Android device to Google so we can see for ourselves what location information is being compiled and transmitted?

4) Is a users' specific location data combined with other information Google collects about users' Internet activities? Is it combined with search data? DoubleClick cookie data? YouTube data, etc.?

5) Regarding "Wi-Fi access points," per your privacy policy, can you describe exactly what information is being collected and for what purpose? Are you collecting just known Wi-Fi access points a device has previously connected to or all Wi-Fi access points in range of the device? Are you collecting just network names or more information like a MAC ID, network address, signal strength or any other information? Are you collecting information about so-called "hot spots," other devices transmitting Wi-Fi signals? Are these Wi-Fi access points stored in a Google database and are they used for identifying a users' specific location?

6) Are there other network signals you are collecting, such as Bluetooth beacons? Again, all Bluetooth signals or only known or paired Bluetooth beacons? Specific device identifiers? Signal strengths?

7) As you know, today's mobile devices contain a range of sensors and consumers may or may not be fully informed about the purpose of those sensors. For example, consumers believe accelerometers are primarily for tracking a users' "steps" within a health app. Do you collect accelerometer data to assist in location tracking? How often and under what circumstances? Consumers believe barometer information is primarily used for "weather" within a weather app. Do you collect barometer information to assist in location tracking? How often and under what circumstances?

8) The Google spokesperson cited in the *Quartz* article stated that "we never incorporated Cell ID into our network sync system." Can you describe exactly what your network sync system is and what information is "incorporated" into it and for what purpose? Does the network sync system include other location-related information?

9) As you know, Google boasts to advertisers that it provides metrics on "store visit conversions" – meaning when a targeted ad translates into a retail store visit. These metrics are "calculated based on aggregated anonymized data from hundreds of millions

of Google users who opt-in to share Location History, click on a search or display ad, then visit a business location."[2] How is Google able to obtain this data if, as was claimed by a Google spokesperson, location data was never used or stored? Specifically, how does Google know when a user visits a business location with "99% accuracy"? Has this location data ever been used to determine if consumers visited a retailer or was influenced by an online/mobile advertisement? If not location, has any other data been used to determine consumer behavior? How exactly are consumers "opting in" to this kind of tracking and use of their data to inform Google store visits conversions?

10) While you commit in the article to cease sending "cell-tower" location data to Google by the end of November, it is not clear if you are also committed to refraining from sending other forms of user location information – whether determined by GPS, Wi-Fi access points, nearby devices, sensors, or any other kind of technology? Can you clarify?

11) Does Google collect user data from Apple iOS devices through Google apps? If so, what data is collected from iOS devices? How is that data collected? Does Google recognize and respect all of the privacy choices made by iOS users? Is Google confident that it is not inadvertently collecting data from consumers who have affirmatively opted out of data collection or location sharing? For example, if a consumer is using Google maps on an Apple device, does Google receive and store that location information?

12) It would seem from the *Quartz* article and your privacy policy that a substantial *quantity* of data is transmitted to Google from Android devices and I assume that occurs on a regular basis. Who is paying for all of this location-related data transmission when a consumer is not using a specific app or not using the Internet? Is this location data transmitted over the cell network, where a consumer is paying for the data? Or just when a user is connected to Wi-Fi? How much information is being transmitted that is not related to a users' specific app or Internet usage and is not for the purposes of diagnostics?

Thank you for your attention to these important questions. The American public is growing increasingly uneasy about the amount of data collected on them. It is important that they are fully aware of exactly when, how, and why their location information is being collected by the companies that they have put their trust in. I respectfully request a response by January 12, 2018.

Sincerely,

Richard Blumenthal
United States Senate

[2] Google AdWords. "Bridging the Customer Journey across the Physical and Digital Worlds." *Google*. static.googleusercontent.com/media/www.google.com/en/us/adwords/start/marketing-goals/pdf/white-paper-bridging-the-customer-journey.pdf .

Attachment 2

Letter from Molinari, Susan (Google). Received by Senators Blumenthal and Markey, 12 Jan. 2018

Google

January 12, 2018

The Honorable Richard Blumenthal
United States Senate
706 Hart Senate Office Building
Washington, D.C., 20510

The Honorable Edward J. Markey
United States Senate
255 Dirksen Senate Office Building
Washington, D.C., 20510

Dear Senator Blumenthal and Senator Markey,

Thank you for your letter of December 1, 2017. We appreciate the opportunity to explain our products and practices and to provide more information about the press report you note.

Privacy and security are critical issues for Google and we are deeply committed to keeping user data private and secure.

We want to be clear, the Quartz story you reference mischaracterizes what happened and how our systems work. The system it described did not use cell tower identifiers ("Cell ID") and never tracked user location. The Quartz article discussed device-side code that is part of a system Google uses to maintain a persistent connection between devices and servers so that the devices can receive notifications and messages in real-time. The system determines the optimal interval at which devices should "ping" servers so that this persistent connection stays open. If the connection closes, messages and notifications may be delayed and users would have to refresh their apps manually to get new messages. This system is designed to help users by determining the optimal ping interval, which helps preserve users' device batteries and makes real-time messaging available.

The claims that Google was using Cell ID from these transmissions to track user location are unfounded and untrue. While the device-side code transmitted data including Mobile Country Code or "MCC", Mobile Network Code or "MNC" and Cell ID, the server-side code (which would not have been accessible to the Quartz reporter) only logged MCC and MNC.

Although the Quartz article incorrectly stated that we were using Cell ID to track users' locations, we do use location data that we collect in other contexts to provide useful products and features to our users such as Google Maps. We welcome the opportunity to answer your additional

questions about how Google and Android work, and have included responses to these questions below.

1. **Google's privacy policy asserts, "When you use Google services, we *may* [emphasis added] collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that *may* [emphasis added], for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers." Under what circumstances "may" Google collect this data? Under what circumstances does Google *always* collect this data? Under what circumstances does Google *never* collect this data?**

We collect and use various types of location information in our products. The types of information we collect depend on a number of factors, including the service we are providing and the user's settings.

For example, standard Internet traffic information, such as IP address, can be used to provide the user with the correct language and locale for search queries. Some products, such as turn-by-turn navigation in Google Maps for mobile, use more precise location information such as GPS signals, device sensors, and Wi-Fi access points when the user has enabled device-based location services.

The Google Location Service (GLS) is the platform network location provider for most Android devices. GLS collects certain kinds of location information (such as Wi-Fi and GPS) from users who have opted into this service on their device and uses that information in an anonymized manner to help improve location accuracy and location-based services. This information also helps determine a device's location, which can be provided to applications that have the necessary location permissions. Users have the ability to opt into GLS when setting up their device or when using an application that uses GLS, and may subsequently disable this collection in their device's location settings at any time.

Location History is a different, Google account-level setting that allows users to store their location information with their Google account in order to get better results and recommendations across Google products. For example, users can see recommendations based on places they have visited with signed-in devices, or traffic predictions for their daily commute. Location History is off by default, and users must opt-in to turn on Location History for their Google account. Users have the ability to control their historical locations saved in their Location History, and can delete all or part of that history at any time.

   a. **What do you mean by "when you use Google services?" Is *all* of Android's operating system a Google service?**

Google plays two roles with respect to data collected on Android. First, Google develops and releases the Android operating system under an open source license, enabling anyone to

access the Android source code and create modified versions of it. In addition, Google develops proprietary mobile applications and services such as Google Play, Search, and Maps (referred to as "Google Mobile Services," or "GMS"), and licenses them separately from Android, meaning that device manufacturers can choose whether and on which devices to install GMS (or can use another mobile OS or suite of comparable apps). These apps, like those created by other developers, run on Android and make use of the platform and other device information to provide services directly to users. The Android operating system on devices with Google apps is a Google service covered by Google's Privacy Policy.

With respect to Android users, therefore, Google may receive information both from their use of Google apps, as well as Google applications installed on the device and services built into Android to make the platform and device function properly (such as the network sync system described below in question 8). Any personal information a user provides to Google, whether through Android system services or Google apps on Android, or that is otherwise generated and stored in a user's Google Account, is used and protected in accordance with the Google Privacy Policy.

This does not mean, however, that Google collects and uses all of the information on an Android device. For example, much of the information that a typical user generates while using Android is collected solely by third party apps running on the platform. As another example, Google enables device manufacturers to modify the open-source Android software such that Google does not receive any information from users of these devices. Information collected by other developers would be subject to their own privacy policies, rather than Google's.

b. What do you specifically mean by "nearby devices?"

With respect to your question on "nearby devices," many connected devices, such as Wi-Fi routers and Bluetooth-enabled devices, are able to detect and connect with each other. Application developers, including Google, may be able to infer a user's location through these connections. For example, if a user has opted into GLS, Google may use publicly broadcast Wi-Fi data from wireless access points in range of the device to help determine its location. As described in more detail below in response to question 5, only publicly broadcast Wi-Fi information is used to estimate the location of a device in this manner.

2. If a user goes "offline" and disconnects their mobile phone from the Internet for a period of time, or even places the device in so-called "airplane mode," does Google receive location data, Wi-Fi data, cell tower data, during this "offline" time period, even if location services is still on?

"Airplane" or "offline" mode is a common setting for mobile devices that disables the device's cellular antenna. When a device is switched into airplane mode, no cellular data, including cell tower data, is sent or received -- however, the device may contain information about the last cellular tower to which it was connected before airplane mode was enabled. A device's Wi-Fi

radio is typically controlled by a separate setting that can be enabled even when a device is in airplane or offline mode, for example to connect to an airplane's Wi-Fi network, or to use the device over a hotel's Wi-Fi network when a user is traveling somewhere without cellular service.

Accordingly, if a user enables airplane or offline mode but leaves on the Wi-Fi radio and connects to a Wi-Fi network, they will be able to continue to send and receive data on their device, including location data, over the Wi-Fi connection. This may include the types of location information described above, depending on the user's settings and the products or services they are using.

3. **What location data does Google specifically collect from Android users and under what circumstances? Is the location data associated with a specific device ID? Is it associated with a specific user ID? Are there any other specific user or device identifiers involved?**

As described above in our response to question 1, the types of location information that Google collects depends on a number of factors, including the service being used and a user's settings. With respect to Android specifically, location information can be used to provide a range of functionality, such as automatic traffic predictions or better search results. Depending on whether and how they want to use these features, users have a number of options for how their location data is collected, including the ability to turn location mode on or off for the device, as well as changing the device's "location accuracy" setting, which controls the sources used to estimate the device's location.

The information Google collects from Android devices for use in GLS is linked to a temporary and rotating device identifier that is not used by or shared with other services. It is not connected with any identifier that would associate that data with a specific user. If a user has opted into Location History, as described above, this location data is stored with their account identifier. Users can control the specific location information saved in their Location History, and can delete their history at any time.

   a. **Can you please attach to your response examples of any relevant files or server logs transmitted by an Android device to Google so we can see for ourselves what location information is being compiled and transmitted?**

With respect to your request for examples of files or logs transmitted by an Android device, we are happy to organize a briefing to determine the specific information that might be most helpful to you.

4. **Is a user's specific location data combined with other information Google collects about users' Internet activities? Is it combined with search data? DoubleClick cookie data? YouTube data, etc.?**

We collect location information in many of our products, and use it along with other information to enhance and improve services for users, and do other things like detect fraud or improve security.

Google Search uses location data to make search results more relevant to the query and the user, and to select ads. For example, searches like "restaurants near me" depend on the device's location to understand what nearby means at that moment. Similarly, a word like "football" usually means something different in the U.S. than it does in the U.K. Some features on the search results page link to licensed content, and for that we try to link the user only to content available in her country. Finally, we use location to serve more relevant ads to that user, similar to the uses for organic search results.

As we describe in our advertiser help center, Google's ad products may receive or infer information about a user's location from a variety of sources. For example, Google may use a user's IP address to identify their general location; receive precise location from a mobile device; or infer a user's location from search queries. In addition, websites or apps a user is using may send information about their location to us. Google uses location information in our ads products to infer demographic information, to improve the relevance of the ads users see, to measure ad performance, and to report aggregate statistics to advertisers. While our systems may use this information to show relevant ads, user location data is not shared with advertisers. For our ad services that operate on partner websites or apps, we may receive more precise location information in an ad request, but we use and store only the general area of the specified location.

YouTube uses a user's location to both personalize the user's watch and recommendations experience, to accurately serve the content licensed to YouTube by content providers, and to target ads. For instance, a user's country will determine what videos they see on the "Trending" tab of YouTube. The "Trending" tab is a set of videos that are rising in popularity in that user's country. For licensing restrictions, YouTube also allows many content owners to select which content is available in which countries. For example, when Disney changed the name of Zootopia to Zootropolis in the U.K., YouTube was able to serve the appropriate trailer to users in the U.K. Finally, as discussed above, YouTube uses a user's location to serve more relevant ads to that user.

Google may also collect and use location information to help detect fraud or other suspicious activity on a user's account. For example, users can review the dates and times on which their accounts have been accessed, as well as the IP address and general location from which these accesses occurred. This enables users to confirm their accounts have not been compromised when unusual activity -- such as an account access from a new country -- is detected.

5. **Regarding "Wi-Fi access points," per your privacy policy, can you describe exactly what information is being collected and for what purpose? Are you collecting just known Wi-Fi access points a device has previously connected to or all Wi-Fi access**

points in range of the device? Are you collecting just network names or more information like a MAC ID, network address, signal strength or any other information? Are you collecting information about so-called "hot spots," other devices transmitting Wi-Fi signals? Are these Wi-Fi access points stored in a Google database and are they used for identifying a user's specific location?

Questions 5(a)-(c) are describing the GLS we provide as a network location provider on Android devices, which uses sources like Wi-Fi and mobile networks to give location information faster and more accurately. When setting up their device or using apps or services that can use location services, a user may enable GLS to take advantage of these features. GLS uses publicly broadcast Wi-Fi data from wireless access points in range of the device to help determine its location. This may include any Wi-Fi access points in range of the device, and not just networks to which the device has previously connected.

These access points are stored and used to build models that estimate where each access point is located. This data is de-identified and only associated with a temporary, rotating device identifier, and no payload data/data packets are collected. As noted above, only publicly broadcast Wi-Fi information is used to estimate the location of a device.

To provide this functionality, Google collects MAC addresses, signal strength information, and radio channel information from these access points. Google also collects the name (also referred to as a "service set identifier" or "SSID") associated with these networks, in order to identify and remove access points that network administrators have chosen to opt out of this collection through instructions provided by Google. SSIDs are discarded after being processed for this purpose.

6. **Are there other network signals you are collecting, such as Bluetooth beacons? Again, all Bluetooth signals or only known or paired Bluetooth beacons? Specific device identifiers? Signal strengths?**

The GLS described above does not use Bluetooth beacon information to determine location.

There are other Google products that may scan and collect certain information from Bluetooth beacons near the device. This includes information that any Bluetooth beacon may be publicly broadcasting for use, such as beacon type, beacon identifier, signal strength, and broadcast power. For example, if a user has turned on the opt-in Location History feature for their Google account, Google will use publicly available beacon information as one signal to help determine location. Other Google products, such as the Nearby service, use Bluetooth scanning to detect nearby Bluetooth beacons in order to show relevant notifications to users when they are near businesses, and other places that have installed Bluetooth beacons for this purpose.

7. **As you know, today's mobile devices contain a range of sensors and consumers may or may not be fully informed about the purpose of those sensors. For example,**

consumers believe accelerometers are primarily for tracking a users' "steps" within a health app. Do you collect accelerometer data to assist in location tracking? How often and under what circumstances? Consumers believe barometer information is primarily used for "weather" within a weather app. Do you collect barometer information to assist in location tracking? How often and under what circumstances?

Many Android devices have built-in sensors that measure motion, orientation, and various environmental conditions. The Android operating system supports a number of these different sensor types, which vary from device to device. These sensors are used to provide a variety of functionality to application developers, such as the ability to measure device movement or positioning to support motion-based games, or to report a compass bearing for a travel application.

Android application developers, including Google, can use the accelerometer and barometer sensors, along with the gyrometer and magnetometer sensors, to more precisely determine a device's location. Google uses the accelerometer readings to help determining the device's orientation and direction, the gyrometer helps determine if a user is turning, and the barometer can help determine the user's elevation.

8. **The Google spokesperson cited in the *Quartz* article stated that "we never incorporated Cell ID into our network sync system." Can you describe exactly what your network sync system is and what information is "incorporated" into it and for what purpose? Does the network sync system include other location-related information?**

The network sync system supports real-time messaging in Google and third party applications on Android mobile devices (*e.g.*, chat apps or notifications). Modern messaging and notification systems allow users to send and receive messages in real-time, so they do not have to "refresh" to see new messages. To do this, it is important for a device to keep its connection to servers alive for as long as possible. If the connection drops, messages will not arrive until the connection is re-established. And a device's battery power is drained when the device attempts to re-establish its connection to the server.

To keep this connection alive, Android devices and servers send pings to each other (referred to as "heartbeats"). If a device does not send a heartbeat ping after a certain period of time, the connection will terminate. For the benefit of users, Google seeks to determine the timing of these heartbeats that best balances the need to maintain a persistent connection between the device and the server with the preservation of device battery. If heartbeats are not frequent enough, connections are lost. If heartbeats are too frequent, battery power is depleted.

Mobile networks have different amounts of traffic and employ different technologies. These factors impact the optimal time interval to wait between each heartbeat. Thus, a device's mobile network provider will impact how frequently a device should send a heartbeat.

Knowing the network to which a device is connected helps Google determine how frequently a device should send a heartbeat ping. Google has access to mobile network information because the information that cell towers transmit to a device includes a MCC (indicating which country the tower is in), a MNC (indicating which cellular network operates the tower), as well as other information like a unique number assigned to each tower (Cell ID). In this instance, the device-side code on Android devices was designed to transmit information from the device that included all three of these data elements. The network sync system also relies on server-side code that determines what information Google actually logs on our servers in connection with the network sync system. This server-side code was written to only log MCC and MNC data for use in the network sync system. Once Google had the MCC and MNC from the device, we aggregated that information and used it to test different ping intervals per country and network in order to determine the optimal ping interval for each network and country.

This heartbeat "tuning" process was the sole reason Google collected the information transmitted by the device-side code at issue; this information was not used to determine user location. In fact, Google never used the Cell ID data from the transmissions to determine user location or, for that matter, ping intervals.

9. **As you know, Google provides metrics on "store visit conversions" -- meaning when a targeted ad translates into a retail store visit. These metrics are "calculated based on aggregated anonymized data from hundreds of millions of Google users who opt-in to share Location History, click on a search or display ad, then visit a business location." How is Google able to obtain this data if, as was claimed by a Google spokesperson, location data was never used or stored? Specifically, how does Google know when a user visits a business location with "99% accuracy"? Has this location data ever been used to determine if consumers visited a retailer or was influenced by an online/mobile advertisement? If not location, has any other data been used to determine consumer behavior? How exactly are consumers "opting in" to this kind of tracking and use of their data to inform Google store visits conversions?**

As explained, Cell ID information was never used to track user location. It is completely unrelated to our Store Visits measurement feature. The Store Visits feature allows retail advertisers to get anonymized and aggregated reports of visits to their retail locations by Google users who also clicked on an ad for the advertiser's products or services. Store visits are measured exclusively using data from Google users who have activated Location History, which provides a location timeline, stored against the user's Google Account. Google correlates the observed store visits from those users who have activated Location History with those users' ad clicks and then uses that data to estimate the aggregate number of store visits for all users who clicked on the advertiser's ads.

Location History is turned off by default, meaning that users must opt-in to this service. Timeline

gives users full control over the locations they choose to keep. Users can pause or delete location history at any time via Timeline.

We provide more information about Store Conversion services in our advertiser help center, which is available at: https://support.google.com/adwords/answer/6361305?hl=en.

10. While you commit in the article to cease sending "cell-tower" location data to Google by the end of November, it is not clear if you are also committed to refraining from sending other forms of user location information -- whether determined by GPS, Wi-Fi access points, nearby devices, sensors, or any other kind of technology? Can you clarify?

By the end of November 2017, Google deactivated the device-side code that transmitted the Cell ID to the network sync system, and that code was changed on each Android device the next time it checked in to receive updates.

As described in our previous answers, other forms of location data are collected and used by Google outside the network sync system, to provide a variety of product and service features.

11. Does Google collect user data from Apple iOS devices through Google apps? If so, what data is collected from iOS devices? How is that data collected? Does Google recognize and respect all of the privacy choices made by iOS users? Is Google confident that it is not inadvertently collecting data from consumers who have affirmatively opted out of data collection or location sharing? For example, if a consumer is using Google maps on an Apple device, does Google receive and store that location information?

Google provides a number of applications for iOS devices, which collect information consistent with Google's Privacy Policy, user controls, and iOS platform rules and settings, including those pertaining to location data.

12. Does anyone pay for location-related data transmission when a consumer is not using a specific app or not using the Internet? If yes, please identify the parties. Is this location data transmitted over the cell network, where a consumer is paying for the data? Or just when a user is connected to Wi-Fi? How much information is being transmitted that is not related to a users' specific app or Internet usage and is not for the purposes of diagnostics?

Data sent and received from Android devices may be transmitted over a Wi-Fi network or over the device's cellular connection. In the case of mobile devices, any charges for transmission of data over a cellular connection -- including any location-related data -- would be governed by a user's mobile carrier plan. The types and quantity of such data that a user's device transmits would depend on the products or services they use, and, in some cases, a user's settings.

Like all operating systems, Android collects diagnostic and other data from user devices to provide and improve system services and device functionality. As we describe above, one such function is the network sync system, which periodically exchanges pings between mobile devices and Google's servers. This helps to maintain a persistent connection so that the devices can send and receive notifications and messages in real-time without having to re-connect to Google's server and deplete battery power.

We appreciate the chance to clarify what happened and how our systems work, as well as explain Google's products and privacy practices. Protecting the privacy and security of our users is a top priority and we thank you for the opportunity to further underscore our commitments in these areas. Please let us know if we can address any other questions you might have or be a resource to you on our shared goals of improving users' mobile experiences and protecting users' privacy and security.

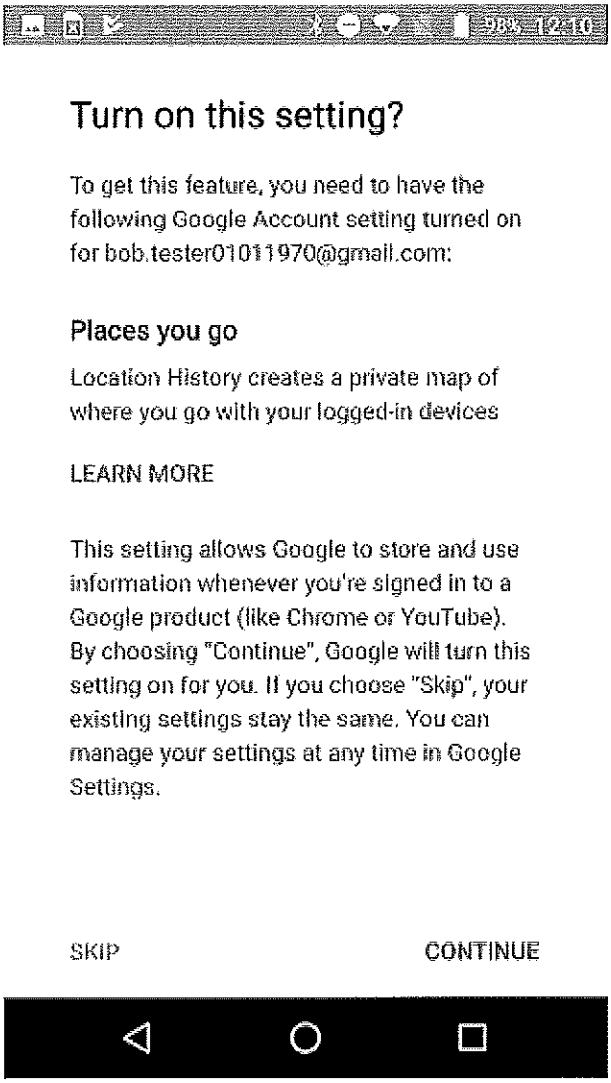
Sincerely,

Susan Molinari
Vice President, Public Policy and Government Relations, Americas
Google

Attachment 3

Google Now Consent Process

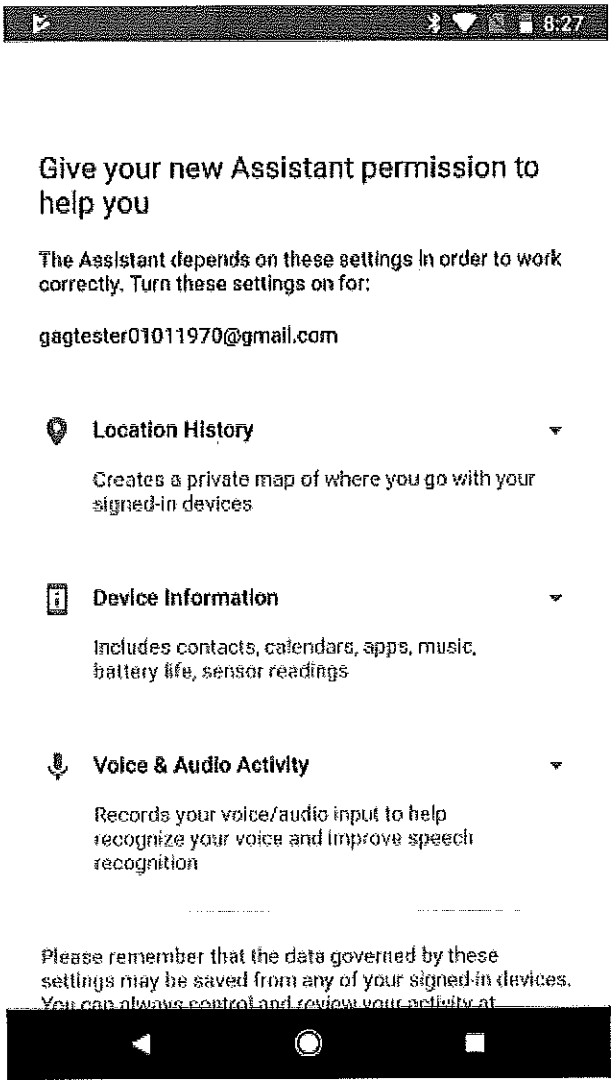
Google Now (from *Quartz*)



Attachment 4

Google Assistance Consent Process

Google Assistant (from *Quartz*)



FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Special Agent Jeremy D'Errico
FBI Richmond Division

Case Number: 91A-RH-3114865

Google Location Geofence Analysis
Area around Call Federal Credit Union
3640 Call Federal Dr, Midlothian, Virginia
May 20, 2019 4:20 PM – 5:20 PM & May 20, 2019 3:50 PM – 5:50 PM

June 17, 2020

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Methods to Determine Mobile Device Location

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Determining Location with GPS

- Global Positioning System (GPS) is a constellation of 24 or more satellites flying 20,350 KM above the surface of the Earth. Each one circles the planet twice a day in one of six orbits to provide continuous worldwide coverage.
- GPS Satellites broadcast radio signals providing their location, status, and precise time from on-board atomic clocks.
- The GPS radio signals travel through space at the speed of light.
- A GPS device receives the radio signals, noting their exact time of arrival, and uses these to calculate its distance from each satellite in view.
- Once a GPS device knows its distance from at least four satellites, it can use geometry to determine its location on Earth in three dimensions.
- "GPS applications typically use a significant amount of power, possibly draining the battery of the [wireless computing device] at an undesirable rate.[2]" – US Patent 9,838,837 – Power-efficient location estimation – Current Assignee: Google LLC.

J.A. 1983

[2]US Patent 9,838,837, "Power-Efficient Location Estimation." Sources: GPS.gov – "How GPS Works" and US Patent and Trademark Office

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Determining Location with WiFi

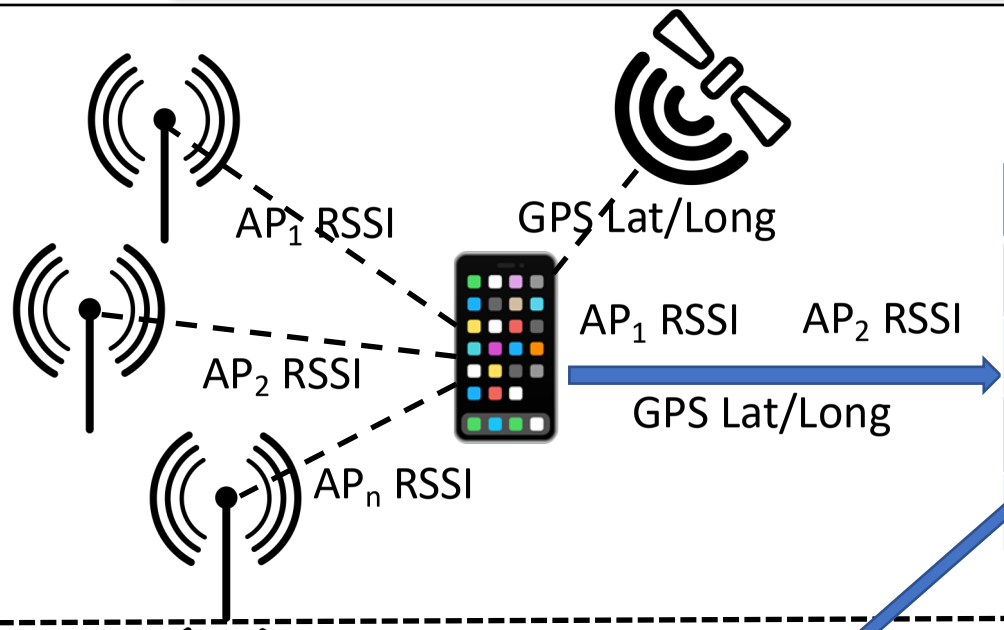
- Mobile device generates a location fingerprint based on scanning for WiFi network devices in the surrounding area.
- Scan includes the MAC (media access control) addresses, signal strengths, and various data of the WiFi network devices (i.e. WiFi access points).
- For each scanned fingerprint location, the mobile device attempts to use GPS to capture current latitude and longitude coordinates.
- On future visits to the location, the mobile device may or may not need to use the GPS based on the success or failure of the previous fingerprint.
- With fingerprinting, the exact location of the reference WiFi access points are not necessary. Connection to the WiFi access point is not required, only the signal strength.
- Google received US Patent number 8,339,316 B1, "Smart GPS Use," on December 25, 2012, and US patent number 10,219,103, "Power-Efficient Location Estimation," on February 26, 2019, which uses fingerprinting of WiFi network devices and GPS to determine location.

J.A. 1984

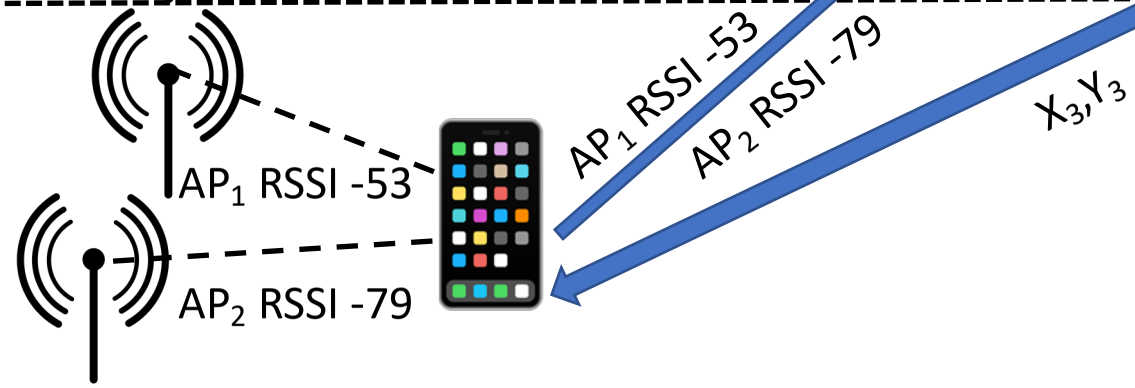
Source: US Patent and Trademark Office

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

WiFi Fingerprinting



Fingerprint	Lat/Long
AP_1 -110; AP_2 -92;	X_1,Y_1
AP_1 -97; AP_2 -92;	X_2,Y_2
AP_1 -53; AP_2 -79;	X_3,Y_3
AP_1 -47; AP_2 -103;	X_n,Y_n



- Google Location Services periodically collects this information in order to determine location.

Source: *On Outdoor Positioning with Wi-Fi*

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Finding Wireless Access Points

Control access point inclusion in Google's Location services

To improve Location services, Google uses publicly broadcast Wi-Fi data from wireless access points and GPS, cell tower, and sensor data. Only publicly broadcast Wi-Fi information is used to estimate the location of a device.

To help apps like Google Maps work better, you can let Google's Location services use your Wi-Fi access point.

Google Location Services

On most Android devices, Google, as the network location provider, provides a location service called Google Location Services (GLS), known in Android 9 as Google Location Accuracy. This service aims to provide a more accurate device location and generally improve location accuracy. Most mobile phones are equipped with GPS, which uses signals from satellites to determine a device's location – however, with Google Location Services, additional information from nearby Wi-Fi, mobile networks, and device sensors can be collected to determine your device's location. It does this by periodically collecting location data from your device and using it in an anonymous way to improve location accuracy.

You can disable Google Location Services at any time in your device's location settings. Your device's location will continue to work even if GLS is turned off, but the device will rely only on GPS to estimate device location for apps with the necessary permission. Google Location Services is distinct from your device's location setting. Learn more

J.A. 1986

Source: Google – Google Maps Help – "Control access point inclusion in Google's Location services" and Google Privacy & Terms – "How Google uses location Information"

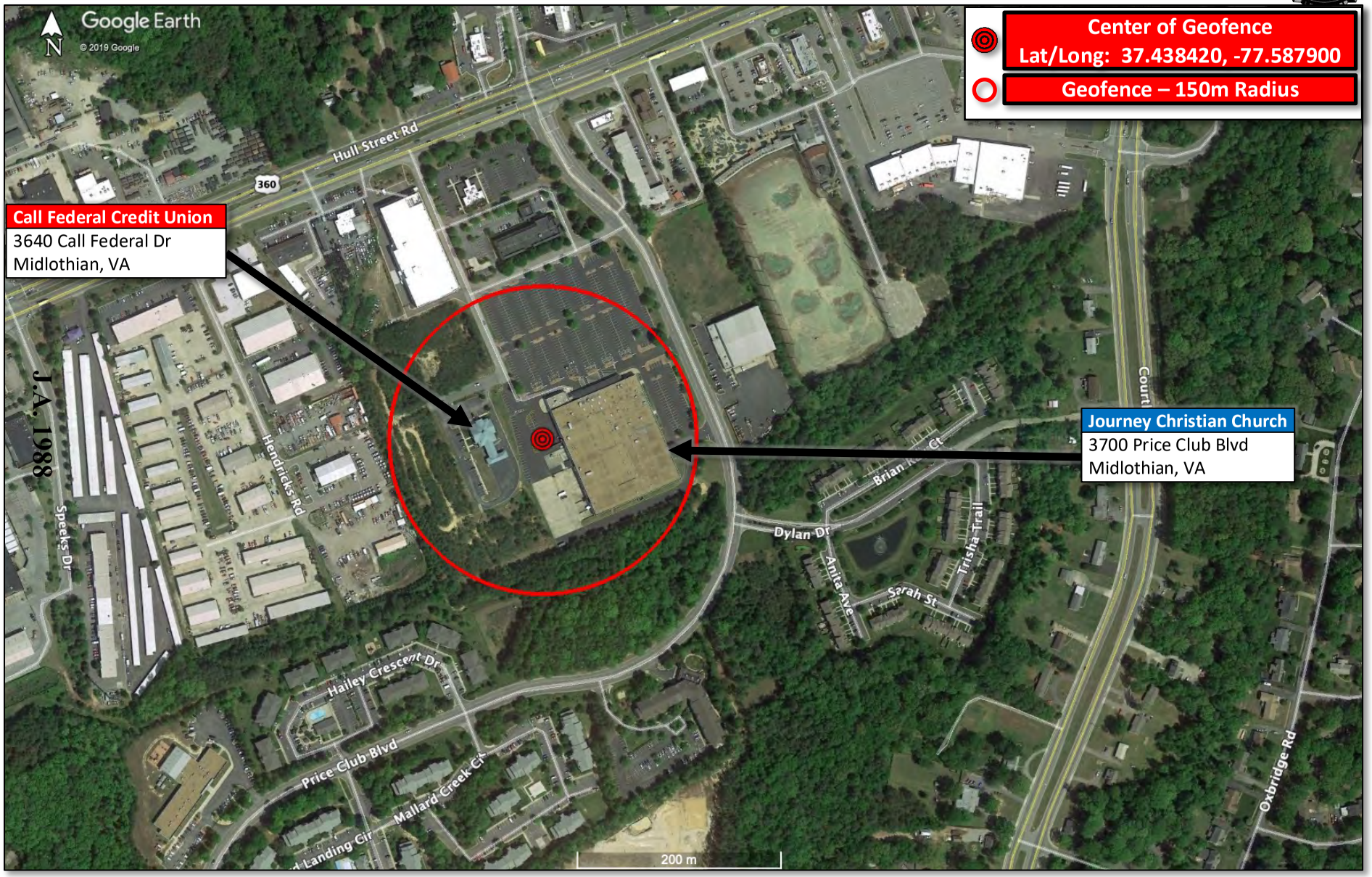
Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Geofence Determination

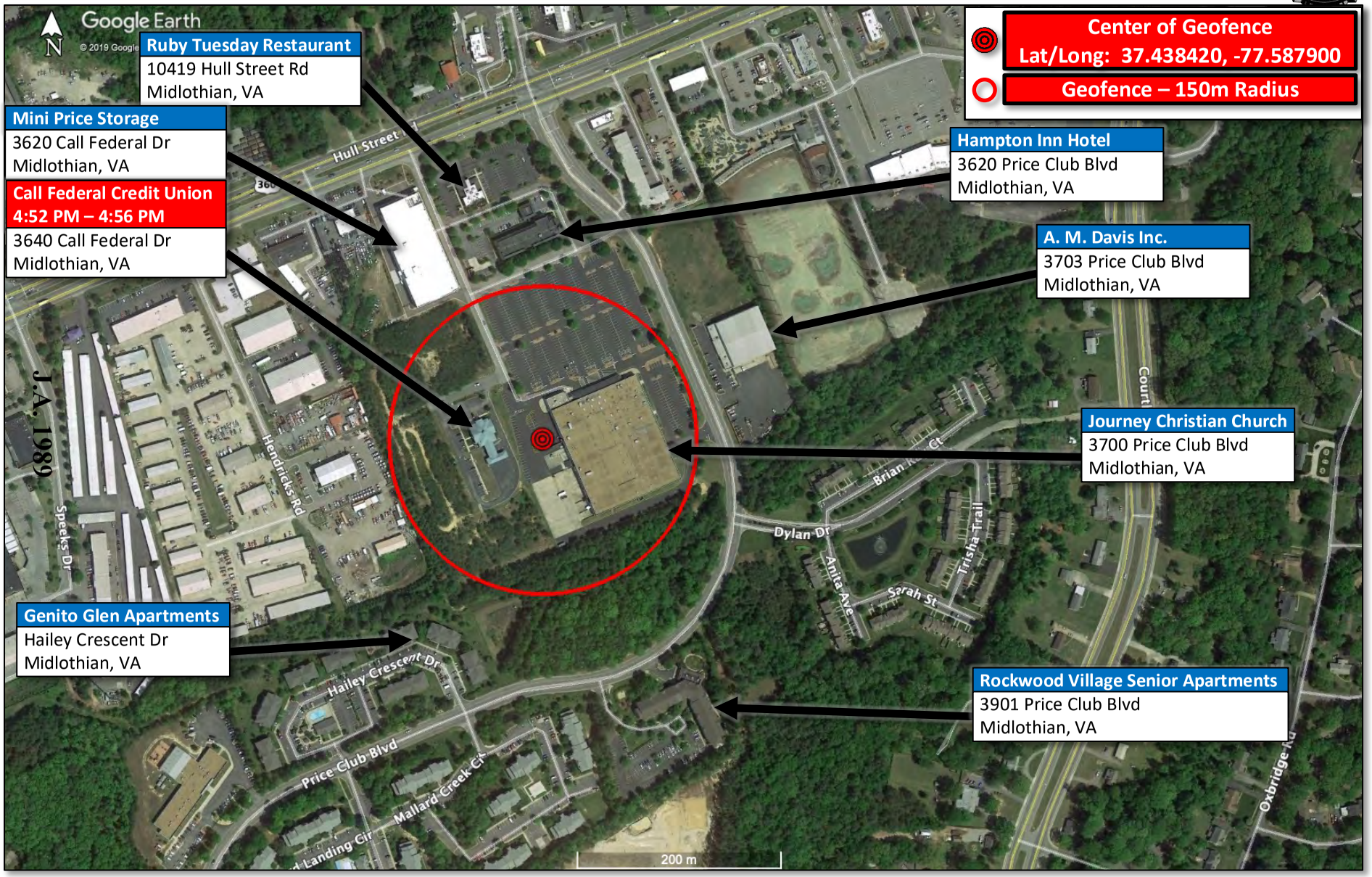
Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Area of Call Federal Credit Union
3640 Call Federal Drive, Midlothian, Virginia

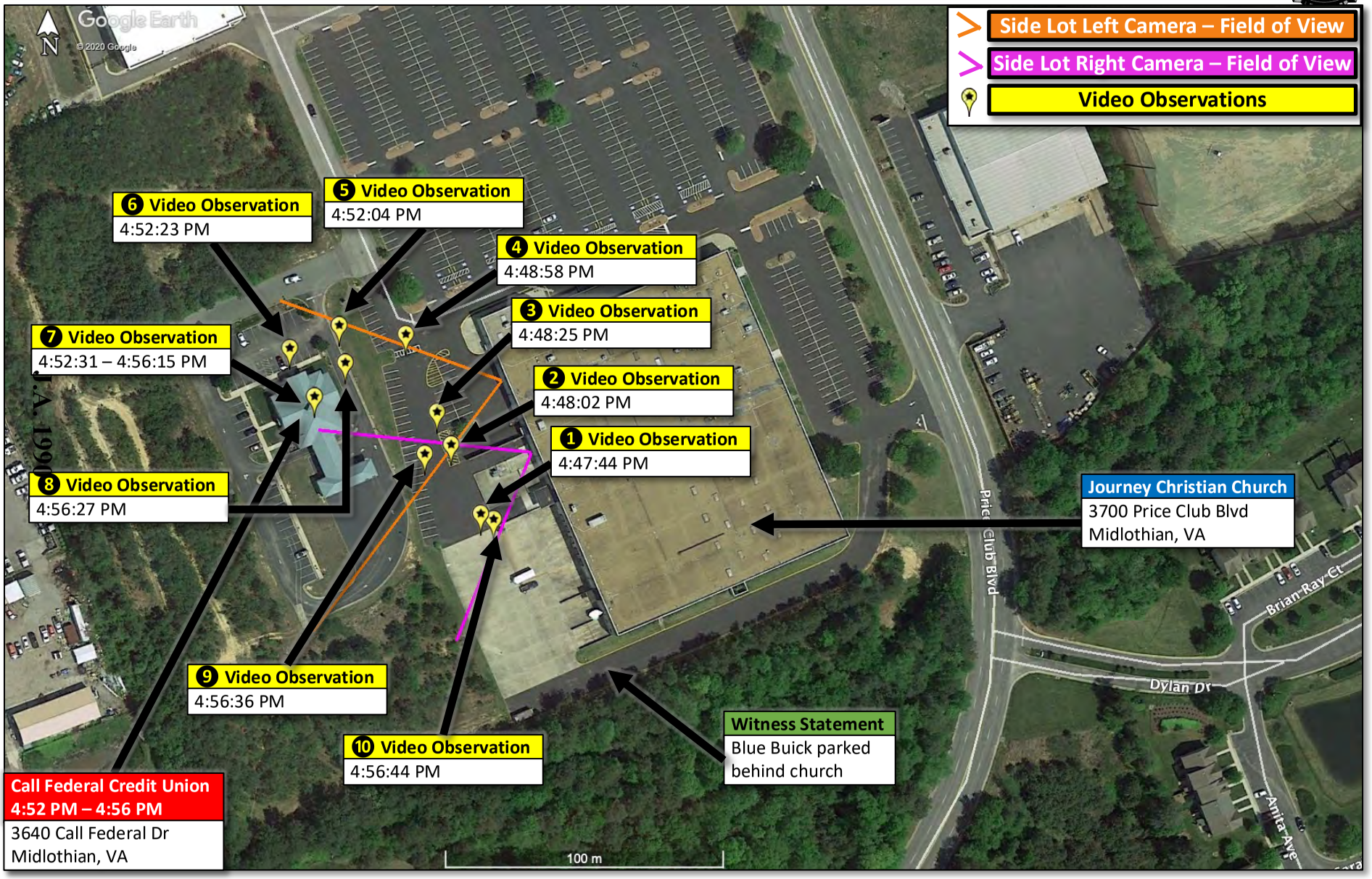


J.A. 1988

Area of Call Federal Credit Union – Surrounding Establishments
3640 Call Federal Drive, Midlothian, Virginia

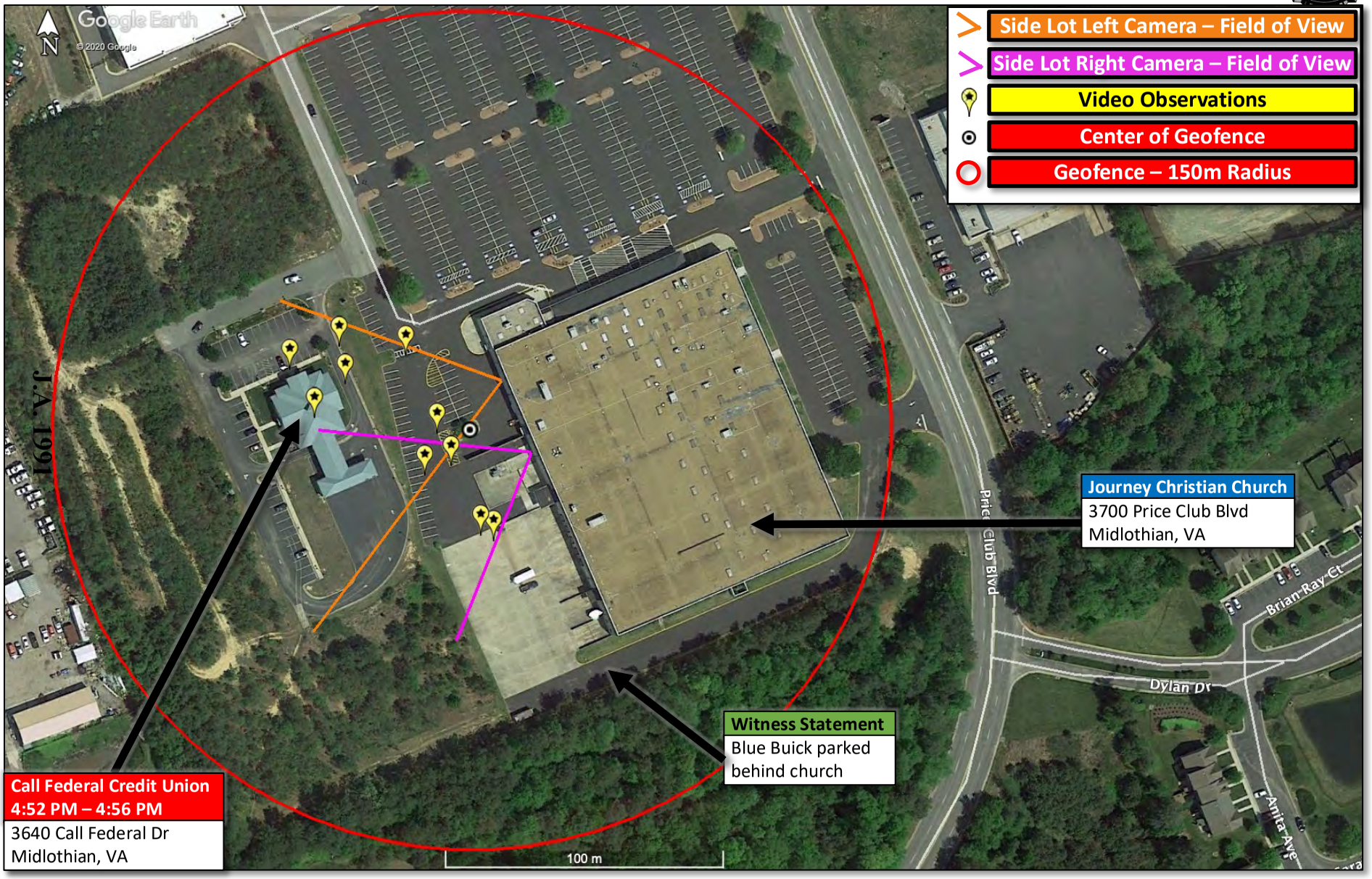


Area of Call Federal Credit Union – Video Observations and Witness Statement
May 20, 2019 4:47 PM – 4:56 PM



 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Area of Call Federal Credit Union – Geofence
May 20, 2019 4:47 PM – 4:56 PM

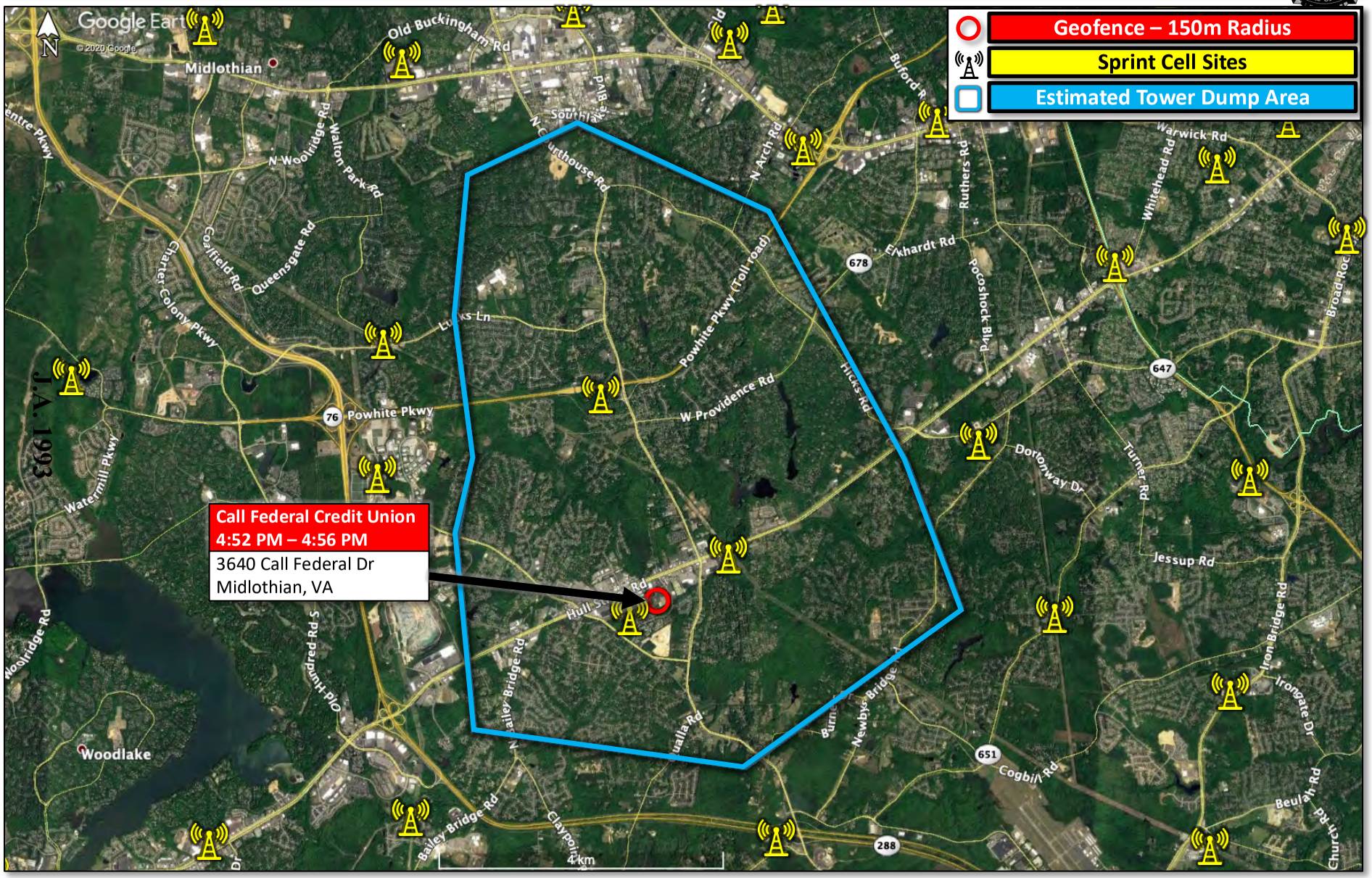


FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Geofence Area vs. Tower Dump Area

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Area of Call Federal Credit Union – Estimated Sprint Tower Dump Coverage Area
May 20, 2019



FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Google Location History Analysis

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Background and Methodology

1. Background

The Federal Bureau of Investigation (FBI) Cellular Analysis Survey Team (CAST) was requested by FBI Task Force Officer (TFO) J. Hylton to analyze Google geofence location history records ("location records") believed to be associated with the armed robbery of the Call Federal Credit Union on or about May 20, 2019.

2. Methodology

An analysis was performed on the location records obtained for the area around the Call Federal Credit Union for the period of May 20, 2019 4:20 PM – 5:20 PM (Stage 1) and location records obtained for selected devices for the period of May 20, 2019 3:50 PM – 5:50 PM (Stage 2).

2.1. Location Records

The location records contained an anonymized device identifier, date, time, latitude, longitude, source, and Maps Display Radius in meters. In order to map the activity associated with the geofence, the location records were imported into mapping software for visualization.

3. Conclusions

An analysis was performed on the location records obtained for this investigation. The methods detailed in Sections 2 and 2.1 were used to produce the attached location analysis maps.

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Google – Types of Accounts

Google Account (personal)

- Access to Google products and services, such as Gmail, Google Drive, Calendar, and Photos.
- Can create an account without Gmail using any email address, such as the email address you have with your organization or another webmail address, such as Yahoo!® or Microsoft® Outlook®.
- Signing up for Gmail automatically creates a Google Account with an @gmail.com address.

G Suite account (for organizations)

- Issued by organization that signed up for G Suite.
- Access to G Suite products and services so you can collaborate with your co-workers.
- Choose from different editions, including G Suite Basic, G Suite Business, G Suite Enterprise, and G Suite for Education, Nonprofits, or Government.
- Provides Android app management through Google Play.

Cloud Identity account (for organizations)

Managed Google Play Accounts (for organizations)

Source: Google – Android Enterprise Help – *Types of Google Accounts*

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Initial Google Geofence Records Provided By Google
First 15 of 209 Records

Example of Records Received from Google

Device ID	Date	Time	Latitude	Longitude	Source	Maps Display Radius (m)
-1144423700	2019/05/20	17:03:50 (-04:00)	37.4385498000	-77.5873707000	WIFI	57
-1144423700	2019/05/20	17:04:27 (-04:00)	37.4386550000	-77.5869634000	WIFI	93
-1144423700	2019/05/20	17:05:03 (-04:00)	37.4386974000	-77.5868483000	WIFI	100
-1144423700	2019/05/20	17:05:39 (-04:00)	37.4386627000	-77.5869429000	WIFI	100
-1144423700	2019/05/20	17:06:01 (-04:00)	37.4385041000	-77.5873436000	WIFI	92
-1305167611	2019/05/20	16:31:26 (-04:00)	37.4384676000	-77.5885140000	WIFI	80
-1305167611	2019/05/20	16:33:27 (-04:00)	37.4384944000	-77.5884743000	WIFI	66
-1305167611	2019/05/20	16:35:29 (-04:00)	37.4385225000	-77.5883613000	WIFI	32
-162381959	2019/05/20	16:21:36 (-04:00)	37.4385755000	-77.5883339000	WIFI	28
-162381959	2019/05/20	16:23:36 (-04:00)	37.4385755000	-77.5883339000	WIFI	28
-162381959	2019/05/20	16:25:38 (-04:00)	37.4385130000	-77.5883798000	WIFI	22
-162381959	2019/05/20	16:27:47 (-04:00)	37.4385130000	-77.5883798000	WIFI	22
-162381959	2019/05/20	16:28:39 (-04:00)	37.4385130000	-77.5883798000	WIFI	22
-162381959	2019/05/20	16:29:24 (-04:00)	37.4385320000	-77.5883830000	WIFI	29
-162381959	2019/05/20	16:31:27 (-04:00)	37.4384951000	-77.5884358000	WIFI	17
...	...	...	...	...	...	...

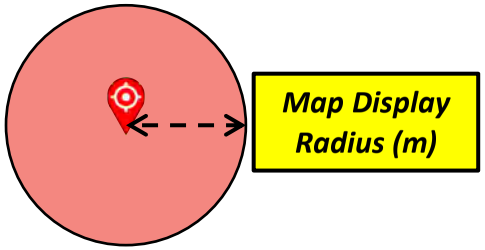
 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Location Records

Location records are illustrated on the subsequent maps using the markers that correspond to the "Source" provided in the location records:

Marker	"Source"
	GPS
	WiFi

The marker indicates the latitude and longitude coordinates provided within the location records. When possible and when appropriate, the marker will be combined with the maps display radius, as shown below.



These symbols will illustrate the approximate location of the mobile device during the time period of analysis.

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

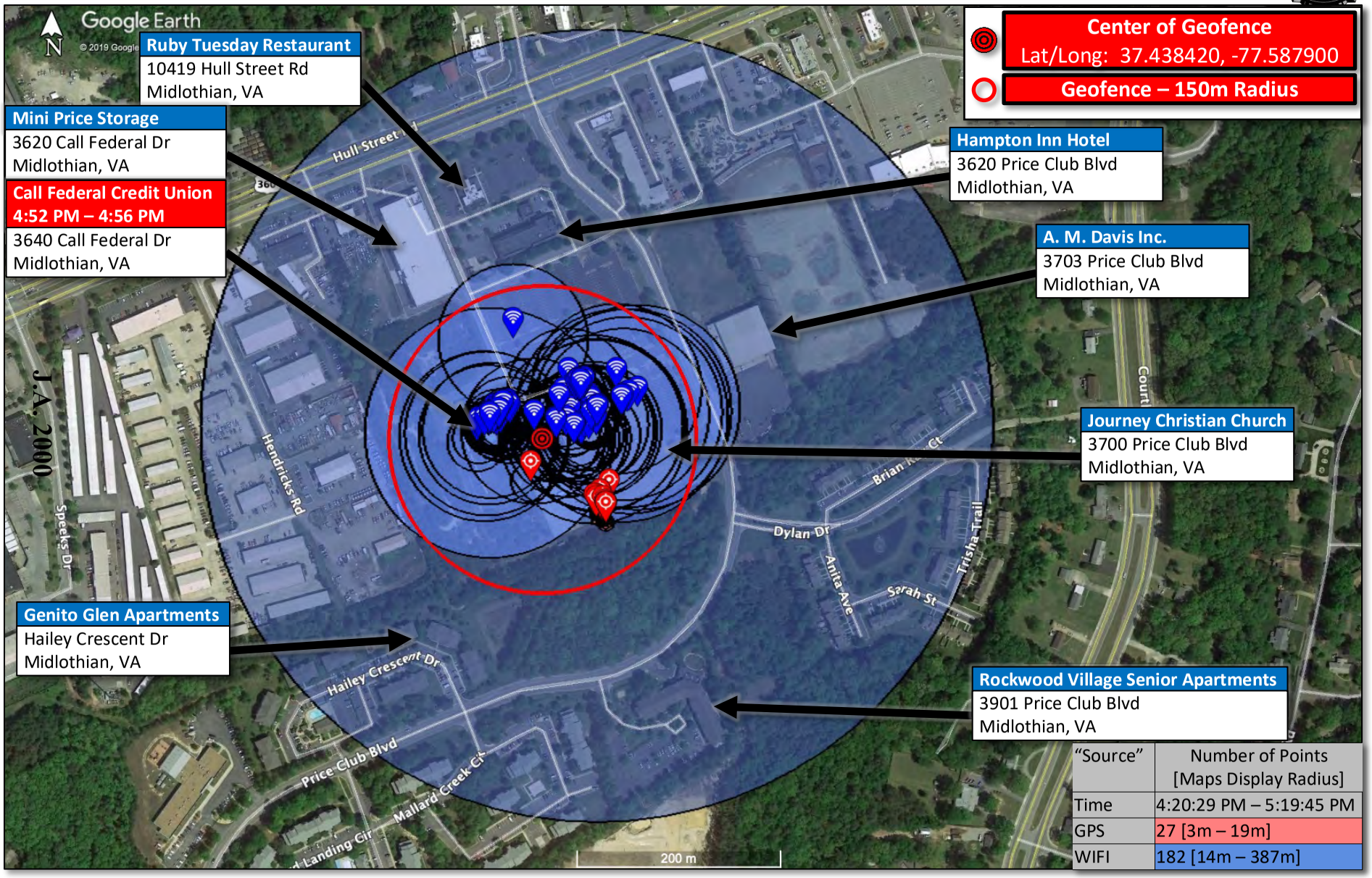
FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Google Location History Analysis

Initial Return from Google

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

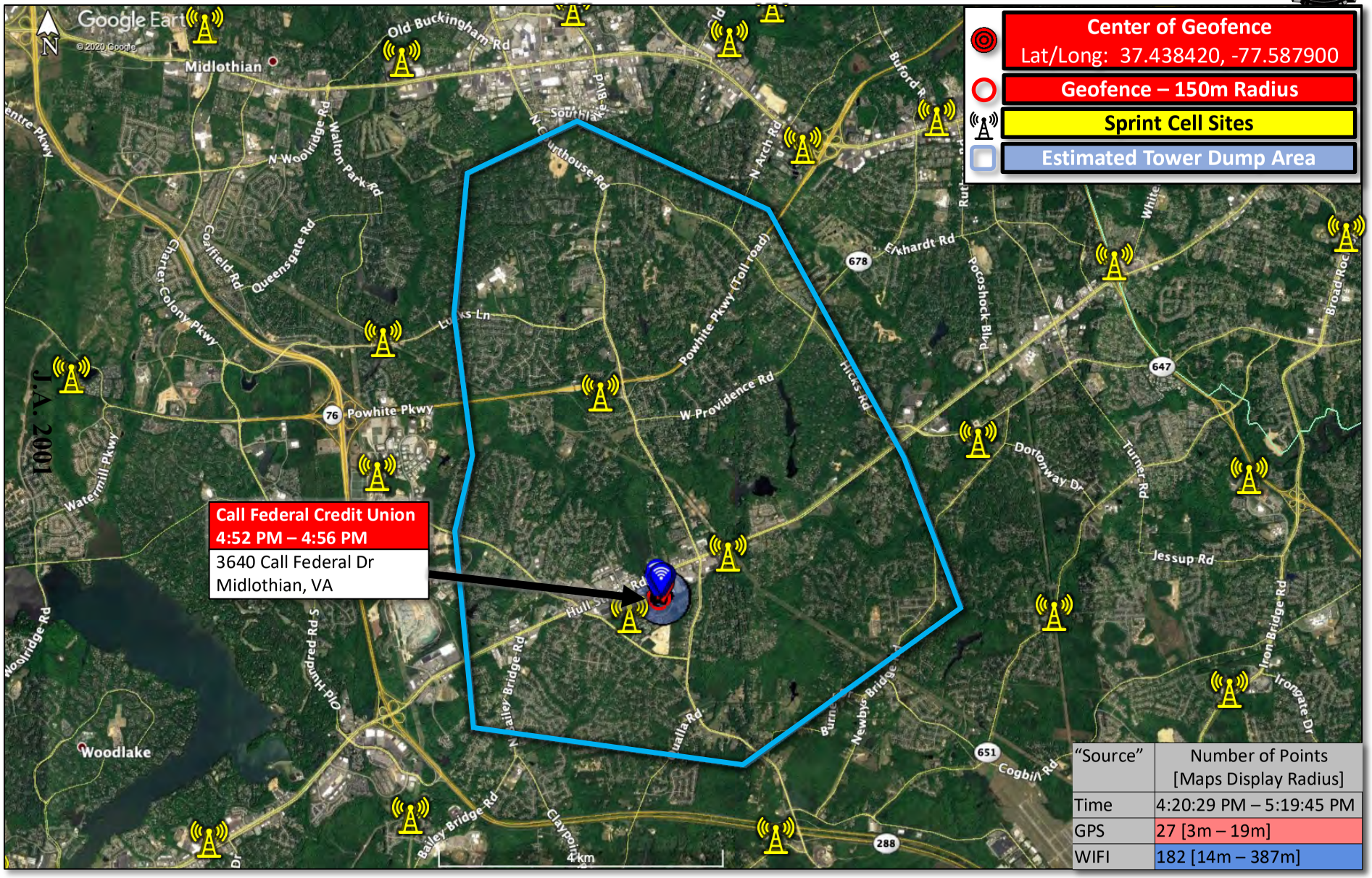
Area of Call Federal Credit Union – May 20, 2019 4:20 PM – 5:20 PM
Initial Google Geofence Records for All Devices



"Source"	Number of Points [Maps Display Radius]
Time	4:20:29 PM – 5:19:45 PM
GPS	27 [3m – 19m]
WIFI	182 [14m – 387m]

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Area of Call Federal Credit Union – May 20, 2019 4:20 PM – 5:20 PM
Initial Google Geofence Records for All Devices Compared to Estimated Sprint Tower Dump Coverage Area



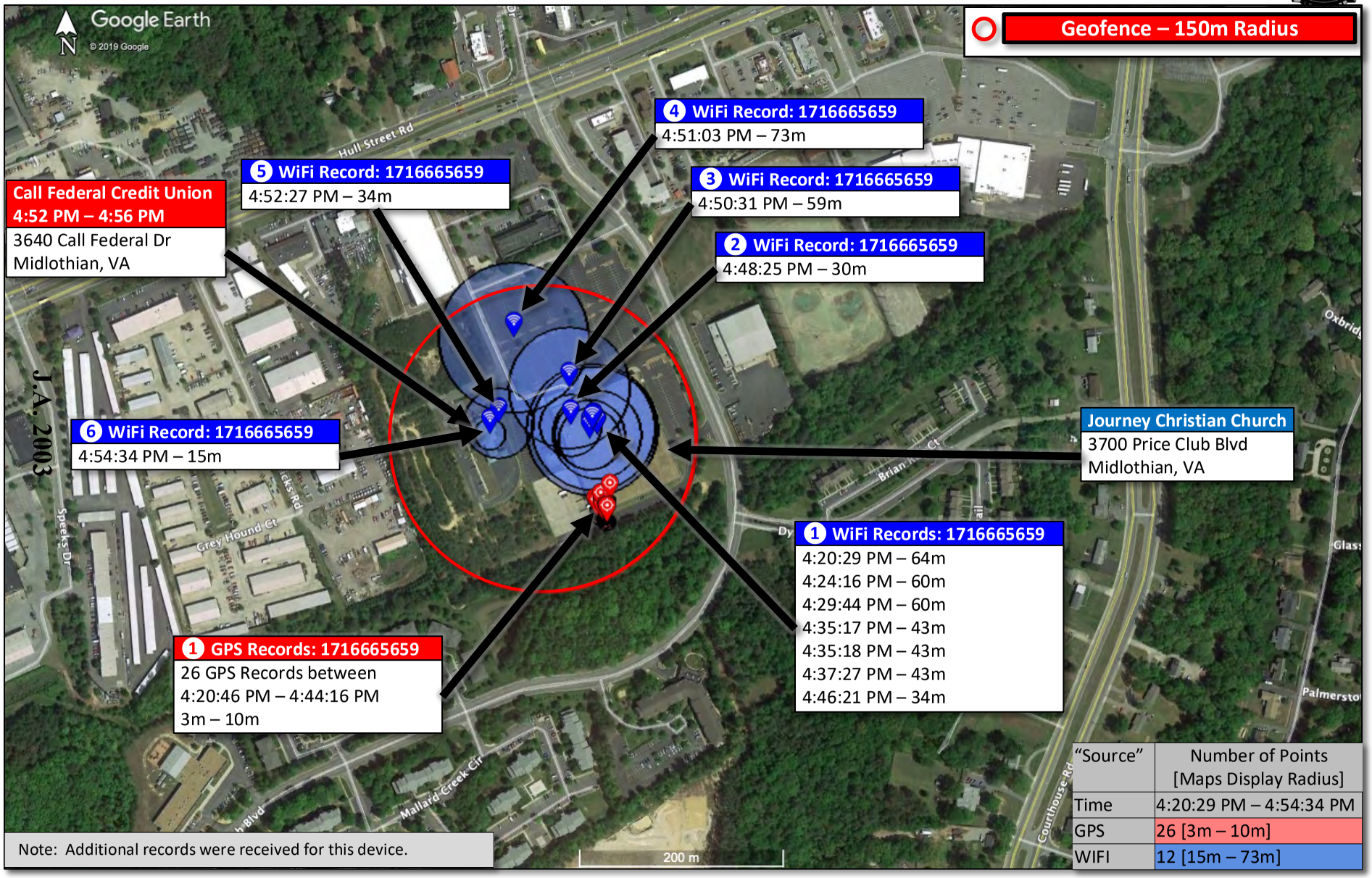
Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Summary of Records Received from Google

Device ID	Number of Records	First Record Time	Last Record Time	Smallest Maps Display Radius (m)	Largest Maps Display Radius (m)	Number of Maps Display Radiuses Extending Beyond Geofence	Maximum Distance Maps Display Radius Extending Beyond Geofence (m)
-2058726931	42	4:30:01 PM	5:19:45 PM	16	45	0	N/A
-1844271119	2	4:20:30 PM	4:22:31 PM	25	66	0	N/A
-1662304683	3	4:44:48 PM	4:47:13 PM	15	68	0	N/A
-1637158857	36	4:21:36 PM	5:18:34 PM	14	42	0	N/A
-1305167611	3	4:31:26 PM	4:35:29 PM	32	80	0	N/A
-1144423700	5	5:03:50 PM	5:06:01 PM	57	100	3	50
-965610516	1	4:41:45 PM	4:41:45 PM	84	84	1	20
-162381959	36	4:21:36 PM	5:18:34 PM	14	42	0	N/A
31133693	7	4:27:38 PM	5:08:26 PM	24	28	0	N/A
138503045	7	4:27:38 PM	5:08:26 PM	24	28	0	N/A
319756533	2	5:17:15 PM	5:19:31 PM	32	71	0	N/A
449021346	1	5:04:45 PM	5:04:45 PM	122	122	1	25
702354289	2	4:29:14 PM	4:29:37 PM	84	387	1	290
907512662	1	4:35:45 PM	4:35:45 PM	84	84	0	N/A
1135979718	1	5:07:02 PM	5:07:02 PM	104	104	1	35
1207269668	5	4:27:40 PM	4:34:43 PM	42	83	0	N/A
1485182252	1	5:04:45 PM	5:04:45 PM	122	122	1	25
1716665659	38	4:20:29 PM	4:54:34 PM	3	73	1	26
2021066118	16	4:23:01 PM	5:02:54 PM	28	83	1	21
Grand Total	**209**	**4:20:29 PM**	**5:19:45 PM**	**3**	**387**	**10**	**290**

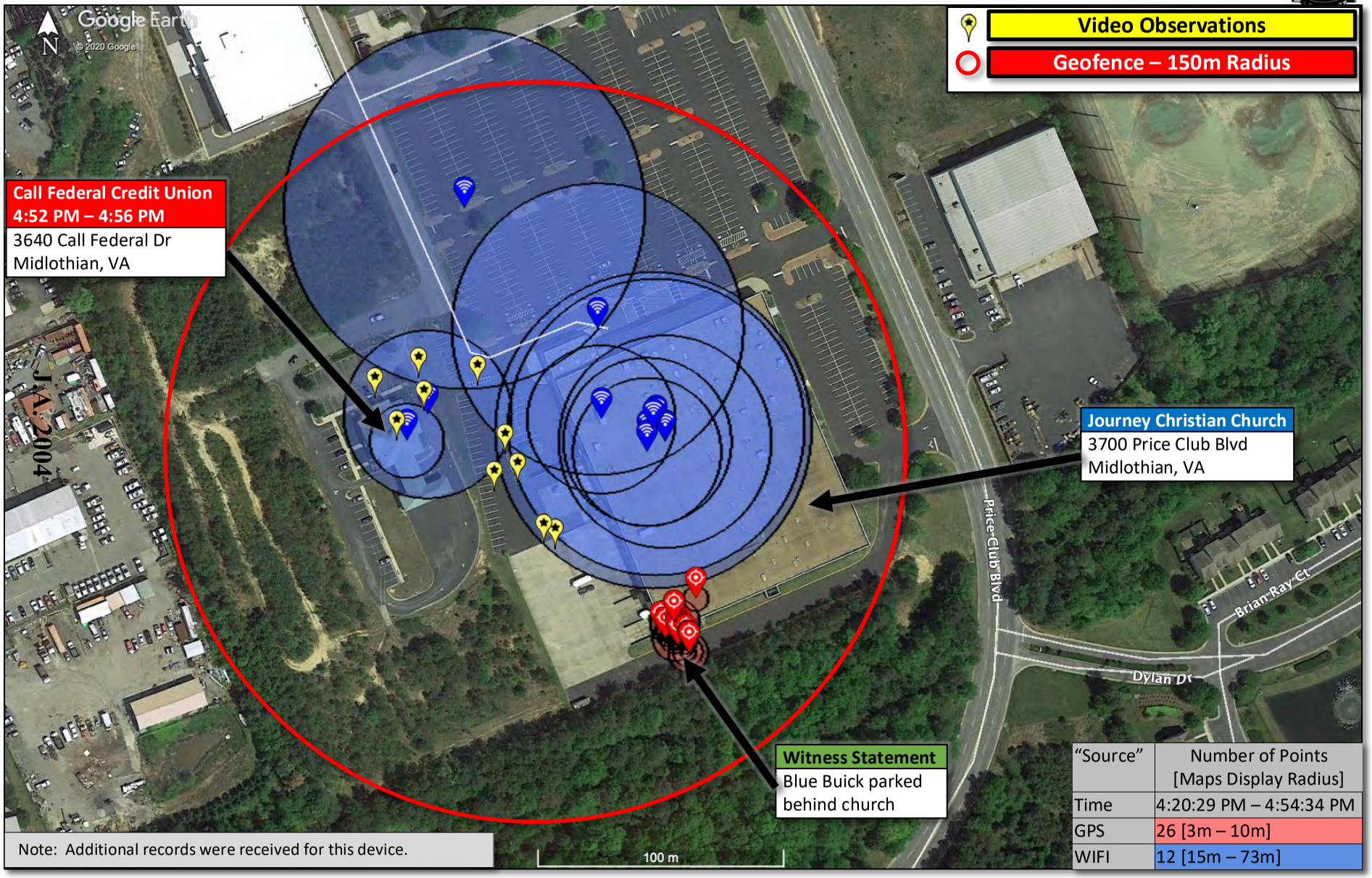
J.A. 2021

Area of Call Federal Credit Union – May 20, 2019 4:20 PM – 5:20 PM
Initial Google Geofence Records for Device ID 1716665659



J.A. 2003

Area of Call Federal Credit Union – May 20, 2019 4:20 PM – 5:20 PM
Initial Google Geofence Records for Device ID 1716665659 with Video Observations and Witness Statement



"Source"	Number of Points [Maps Display Radius]
Time	4:20:29 PM – 4:54:34 PM
GPS	26 [3m – 10m]
WIFI	12 [15m – 73m]

Note: Additional records were received for this device.

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Google Location History Analysis

Supplemental Return from Google

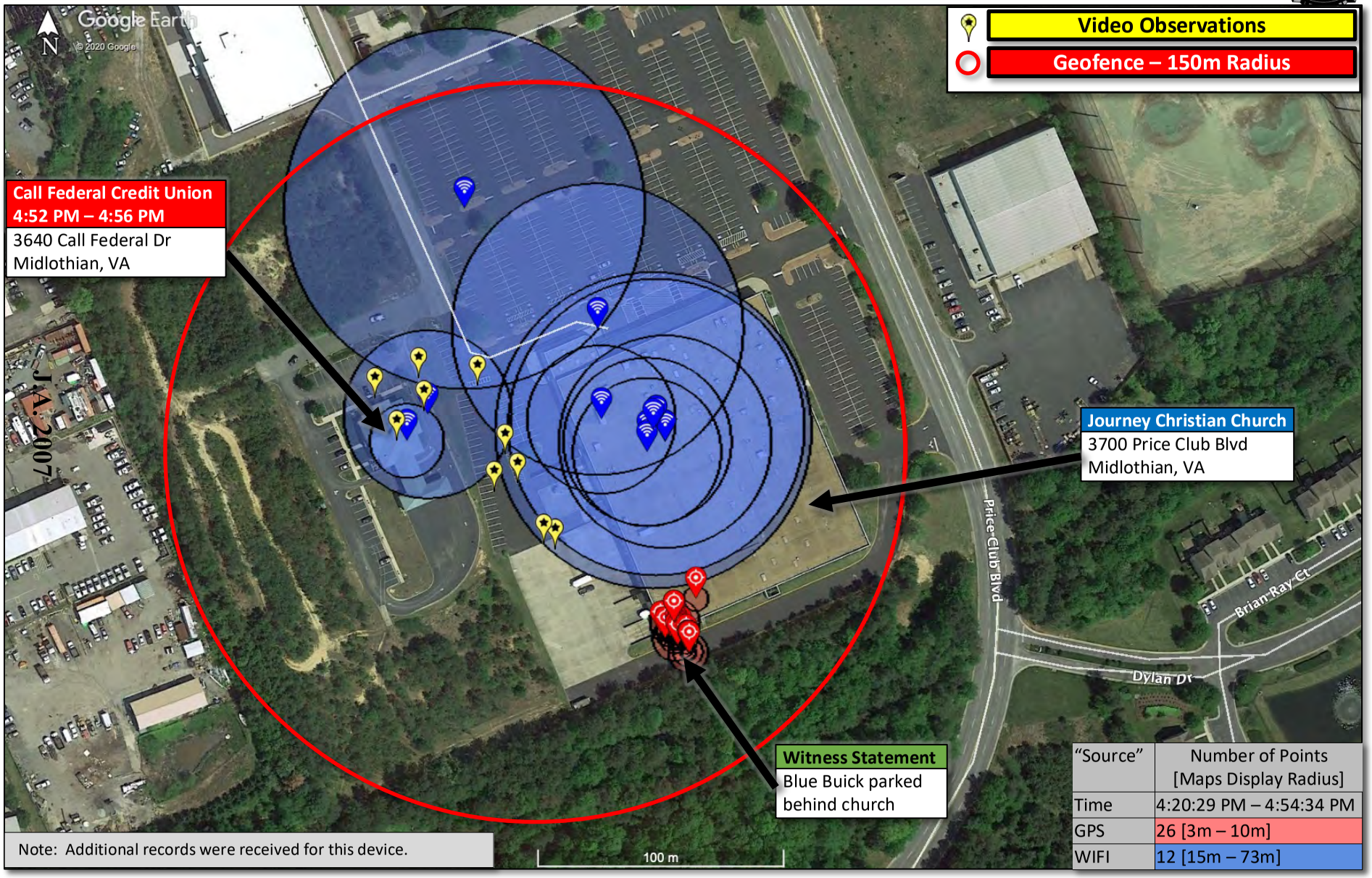
Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Summary of Records Received from Google

Device ID	Number of Records	First Record Time	Last Record Time	Smallest Maps Display Radius (m)	Largest Maps Display Radius (m)
-1844271119	29	3:50:10 PM	5:29:25 PM	16	100
-1662304683	56	3:55:04 PM	5:49:08 PM	4	1,842
-1305167611	63	3:51:29 PM	5:49:23 PM	10	210
-965610516	56	3:50:11 PM	5:48:27 PM	4	1,026
702354289	183	3:50:59 PM	5:49:47 PM	6	387
907512662	64	3:55:11 PM	5:45:36 PM	14	413
1207269668	90	3:53:16 PM	5:45:26 PM	16	164
1716665659	94	3:53:10 PM	5:48:46 PM	3	1,797
2021066118	45	3:51:24 PM	5:49:26 PM	6	1,838
Grand Total	**680**	**3:50:10 PM**	**5:49:47 PM**	**3**	**1,842**

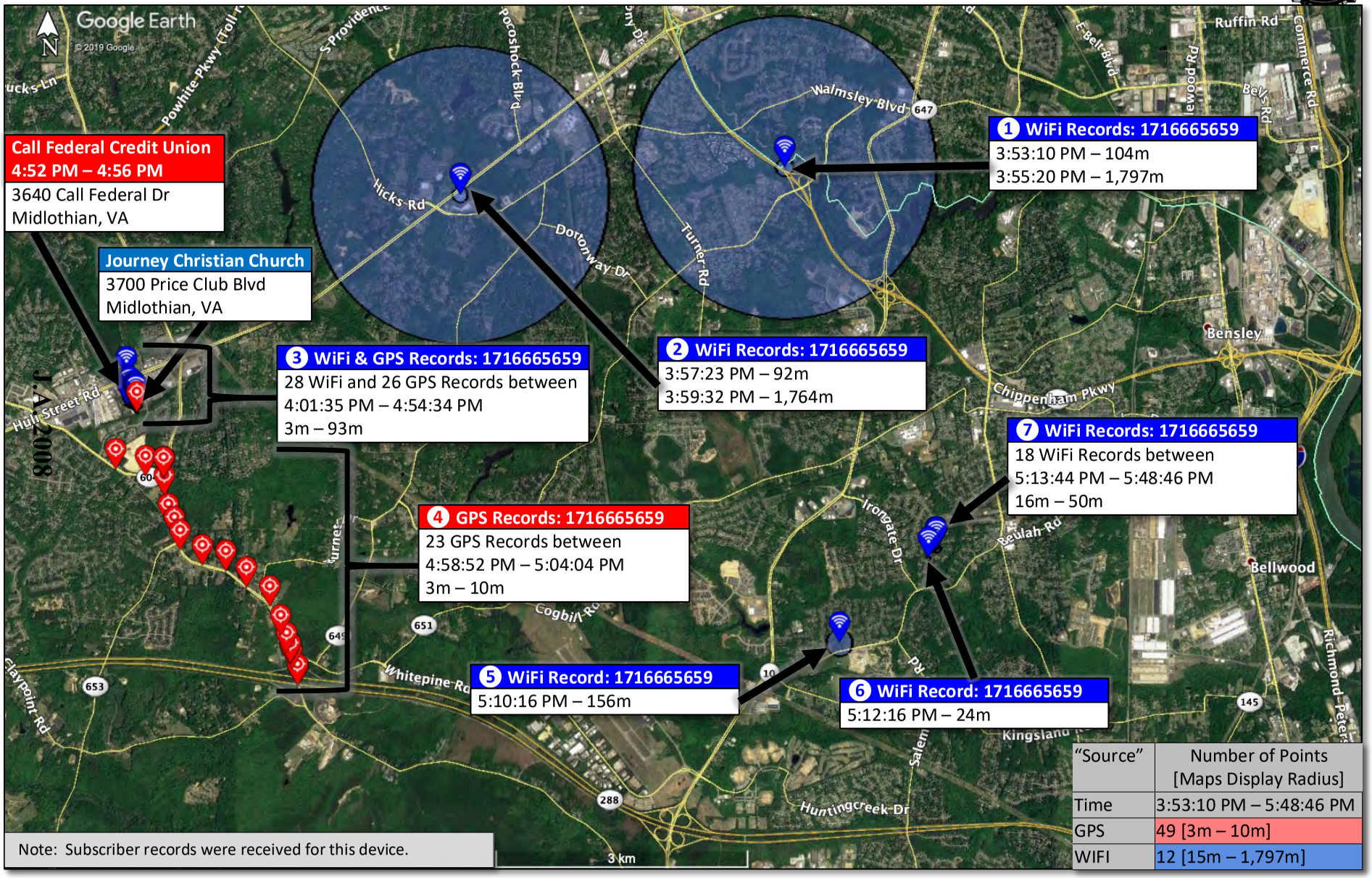
 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Area of Call Federal Credit Union – May 20, 2019 4:20 PM – 5:20 PM
Initial Google Geofence Records for Device ID 1716665659 with Video Observations and Witness Statement



Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

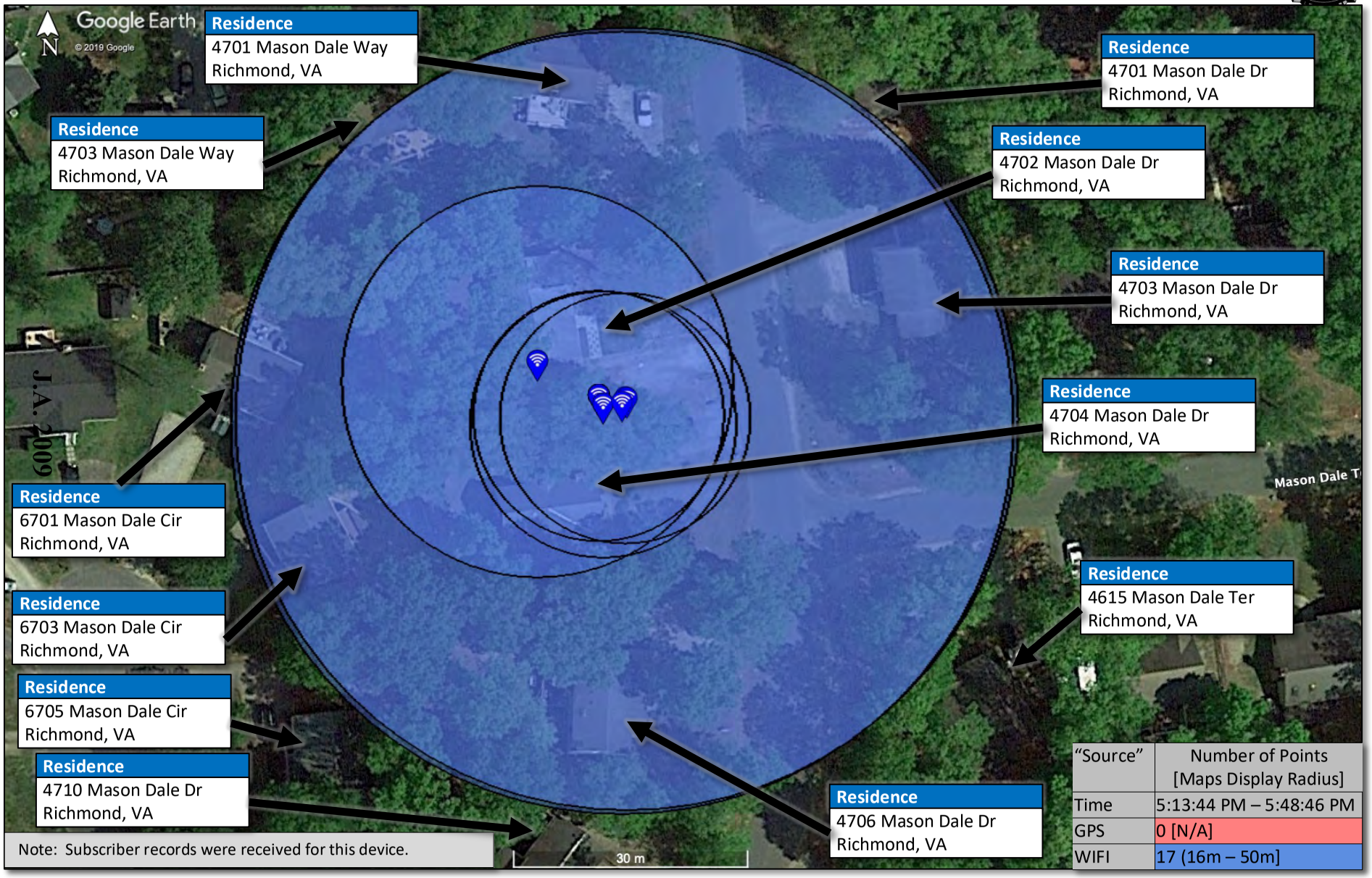
Area of Call Federal Credit Union – May 20, 2019 3:50 PM – 5:50 PM
Supplemental Google Geofence Records for Device ID 1716665659



"Source"	Number of Points [Maps Display Radius]
Time	3:53:10 PM – 5:48:46 PM
GPS	49 [3m – 10m]
WIFI	12 [15m – 1,797m]

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Area of Mason Dale Drive – May 20, 2019 5:13 PM – 5:50 PM
Supplemental Google Geofence Records for Device ID 1716665659



Note: Subscriber records were received for this device.

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Google Location History Analysis

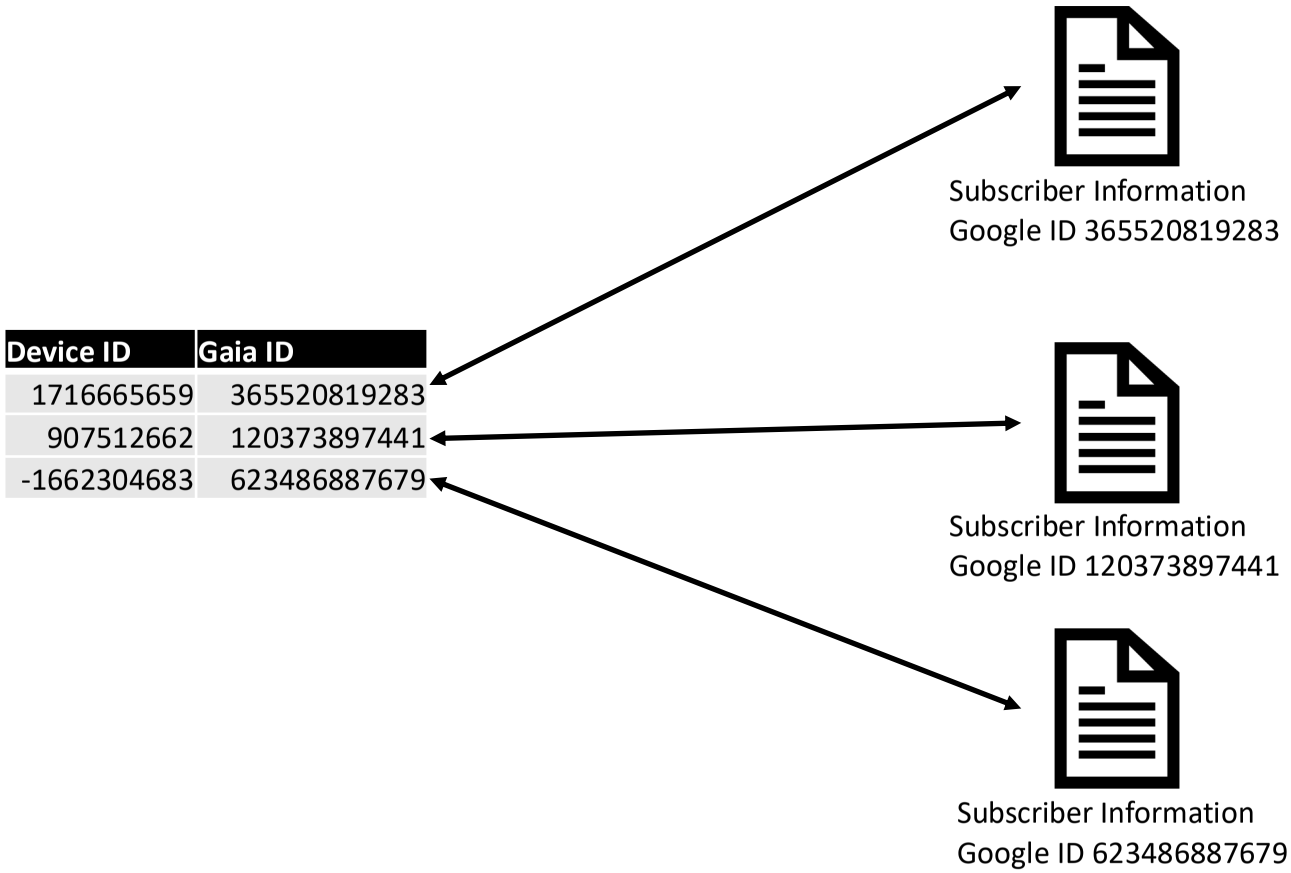
Subscriber Information from Google

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Summary of Subscriber Information Provided By Google
Google Geofence Records

J.A. 2011

Device ID	Gaia ID
1716665659	365520819283
907512662	120373897441
-1662304683	623486887679



Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Subscriber Information Provided By Google
Google Geofence Records for Device ID 1716665659

Subscriber Information Key Provided by Google for Requested Device IDs

Gaia ID	Device ID
365520819283	1716665659
120373897441	907512662
623486887679	-1662304683

############### * Google Confidential and Proprietary * ###############

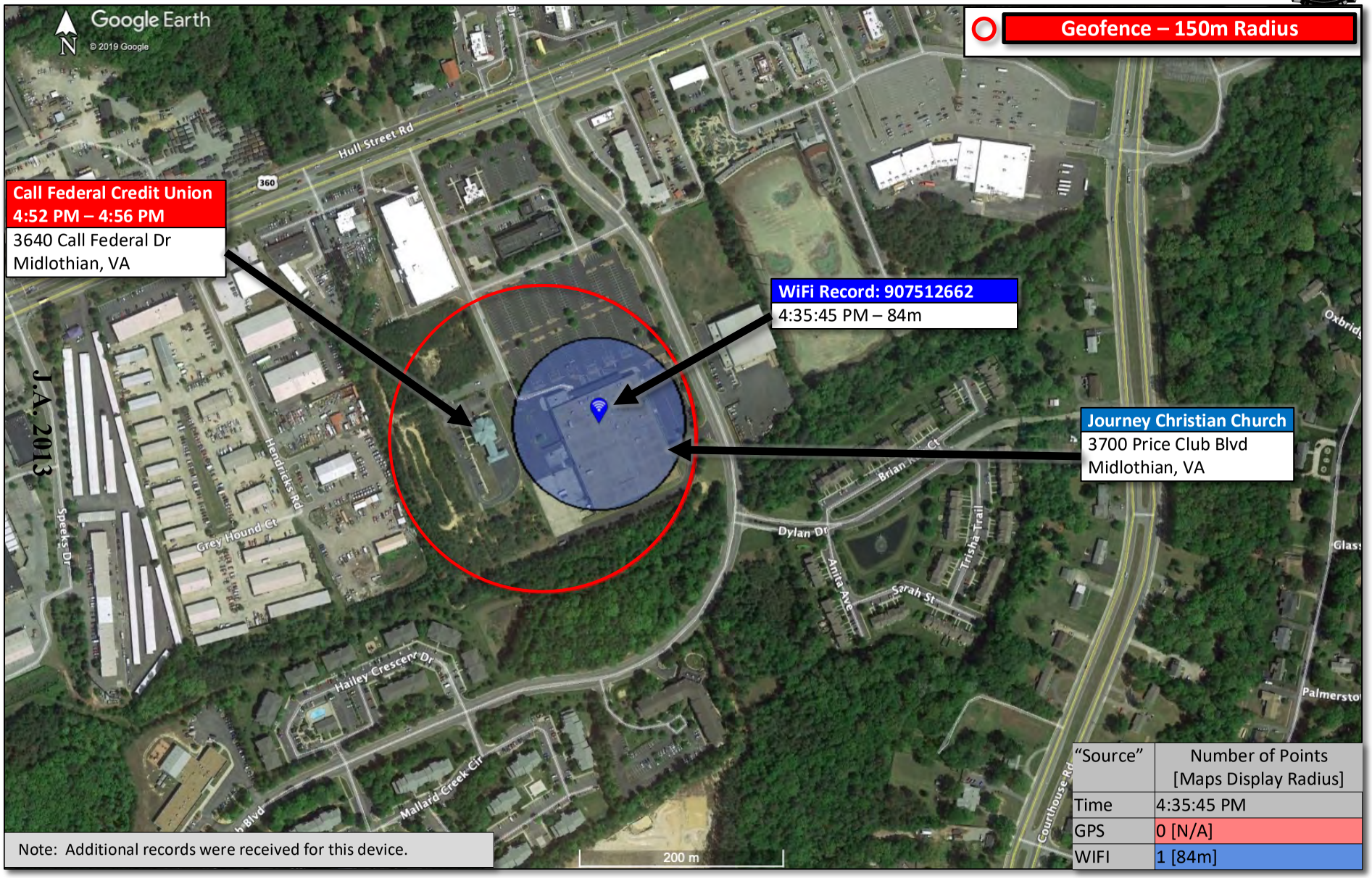
GOOGLE SUBSCRIBER INFORMATION
Name: jamaican media
e-Mail: okellochatrie55@gmail.com
Status: Enabled
Services: Android, Gmail, Google Calendar, Google Hangouts, Google My Maps, Google Payments, Google Play, Location History, Minutemaid, Web & App Activity, YouTube
Recovery e-Mail: okellochatrie0@gmail.com
Created on: 2017/08/20-18:04:11-UTC
Terms of Service IP: 71.115.30.129, on 2017/08/20-18:04:11-UTC
Language Code: en
Google Account ID: 365520819283
Last Logins: 2019/05/20-13:49:12-UTC, 2019/05/20-11:49:16-UTC, 2019/05/20-01:24:44-UTC

Time	IP Address	Type
5 consecutive Login events from IP 2601:5c2:4400:7ca:5c1b:4e:9baa:f09b occurred during past 24 hours prior to the following event.		
2019/05/20-13:49:12-UTC	2601:5c2:4400:7ca:5c1b:4e:9baa:f09b	Login

############### * Google Confidential and Proprietary * ###############

Jul 2021

Area of Call Federal Credit Union – May 20, 2019 4:20 PM – 5:20 PM
Initial Google Geofence Records for Device ID 907512662

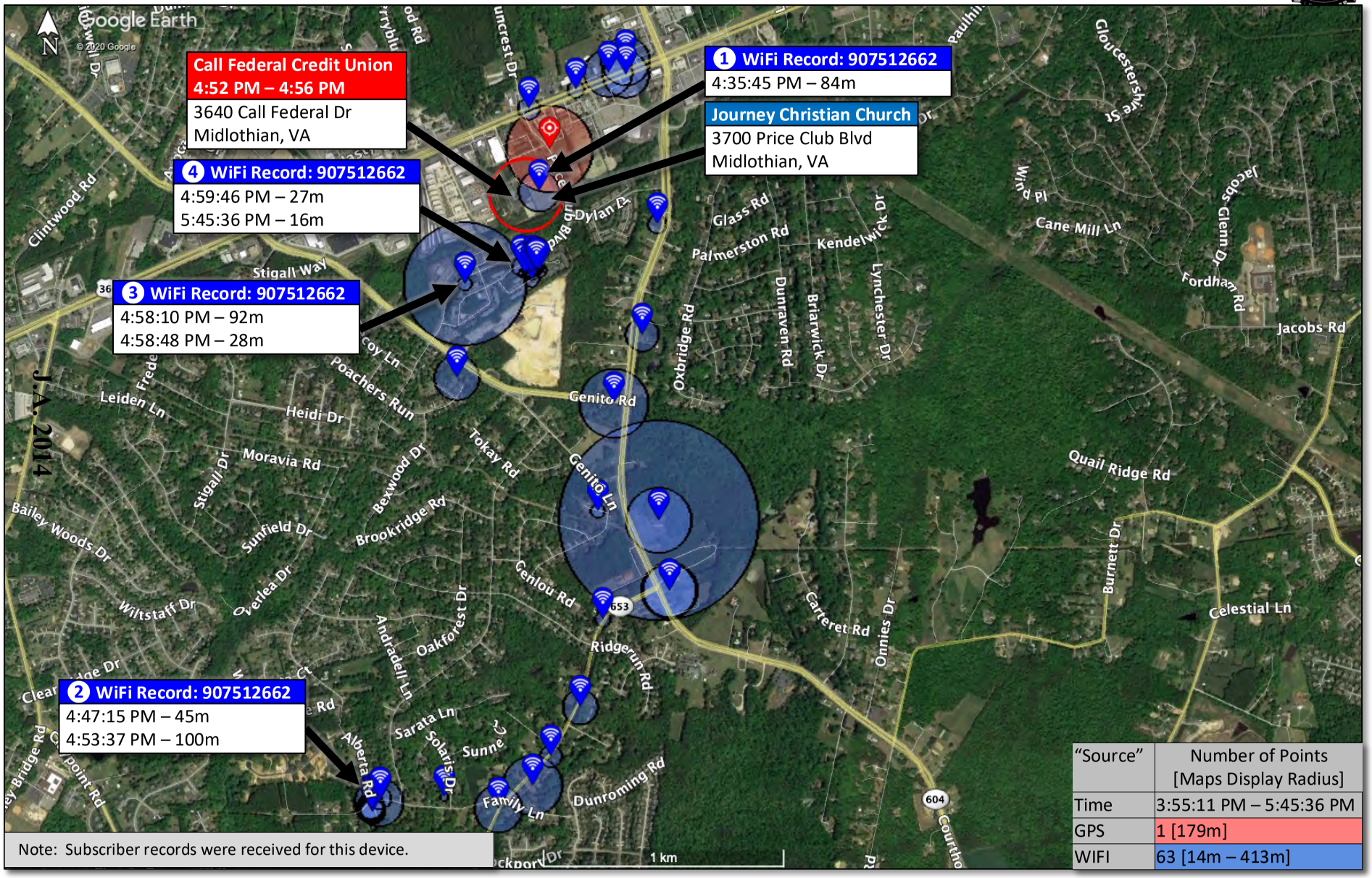


"Source"	Number of Points [Maps Display Radius]
Time	4:35:45 PM
GPS	0 [N/A]
WIFI	1 [84m]

J.A. 2013

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Area of Call Federal Credit Union – May 20, 2019 3:50 PM – 5:50 PM
Supplemental Google Geofence Records for Device ID 907512662

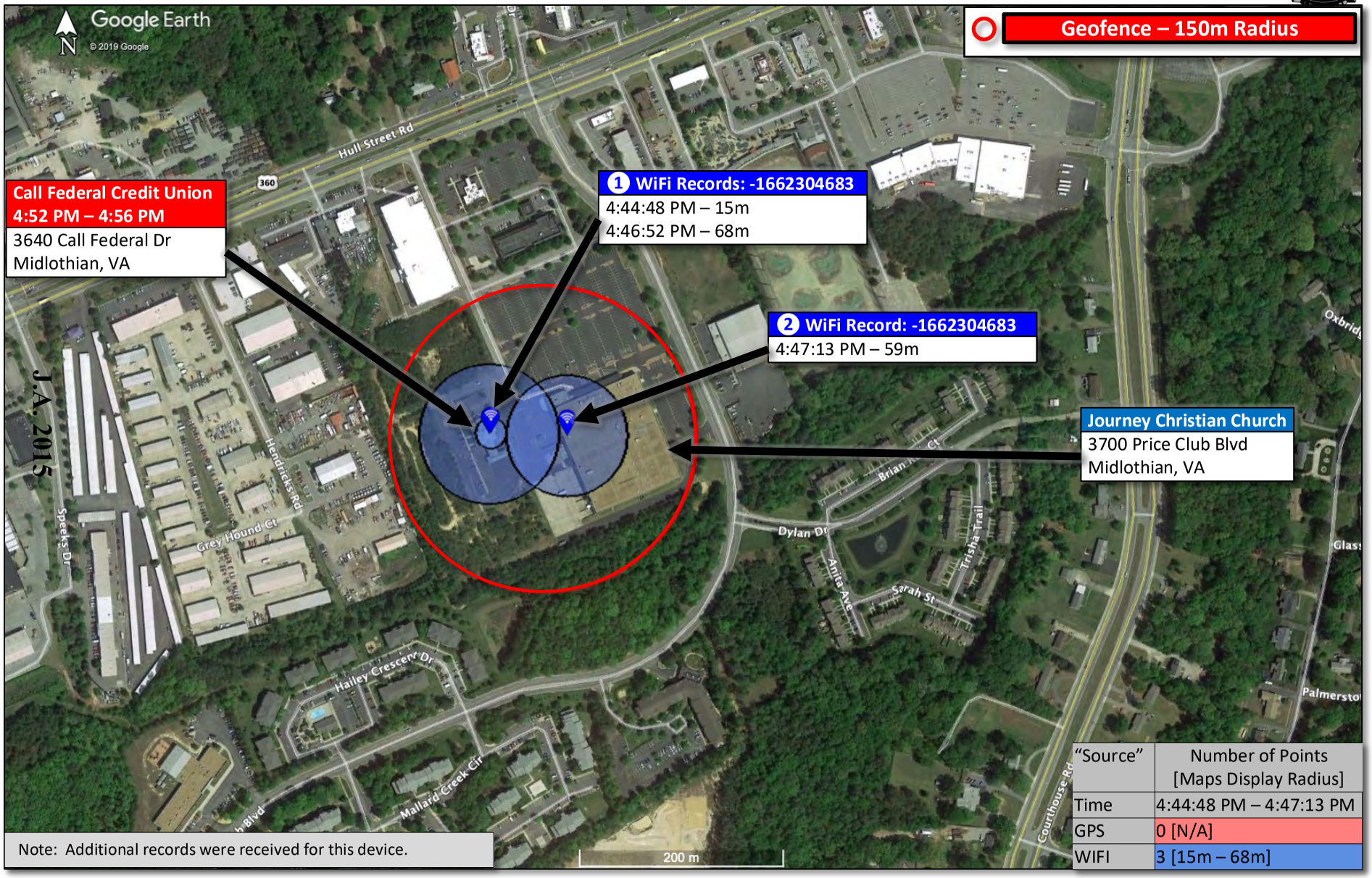


Note: Subscriber records were received for this device.

"Source"	Number of Points [Maps Display Radius]
Time	3:55:11 PM – 5:45:36 PM
GPS	1 [179m]
WIFI	63 [14m – 413m]

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

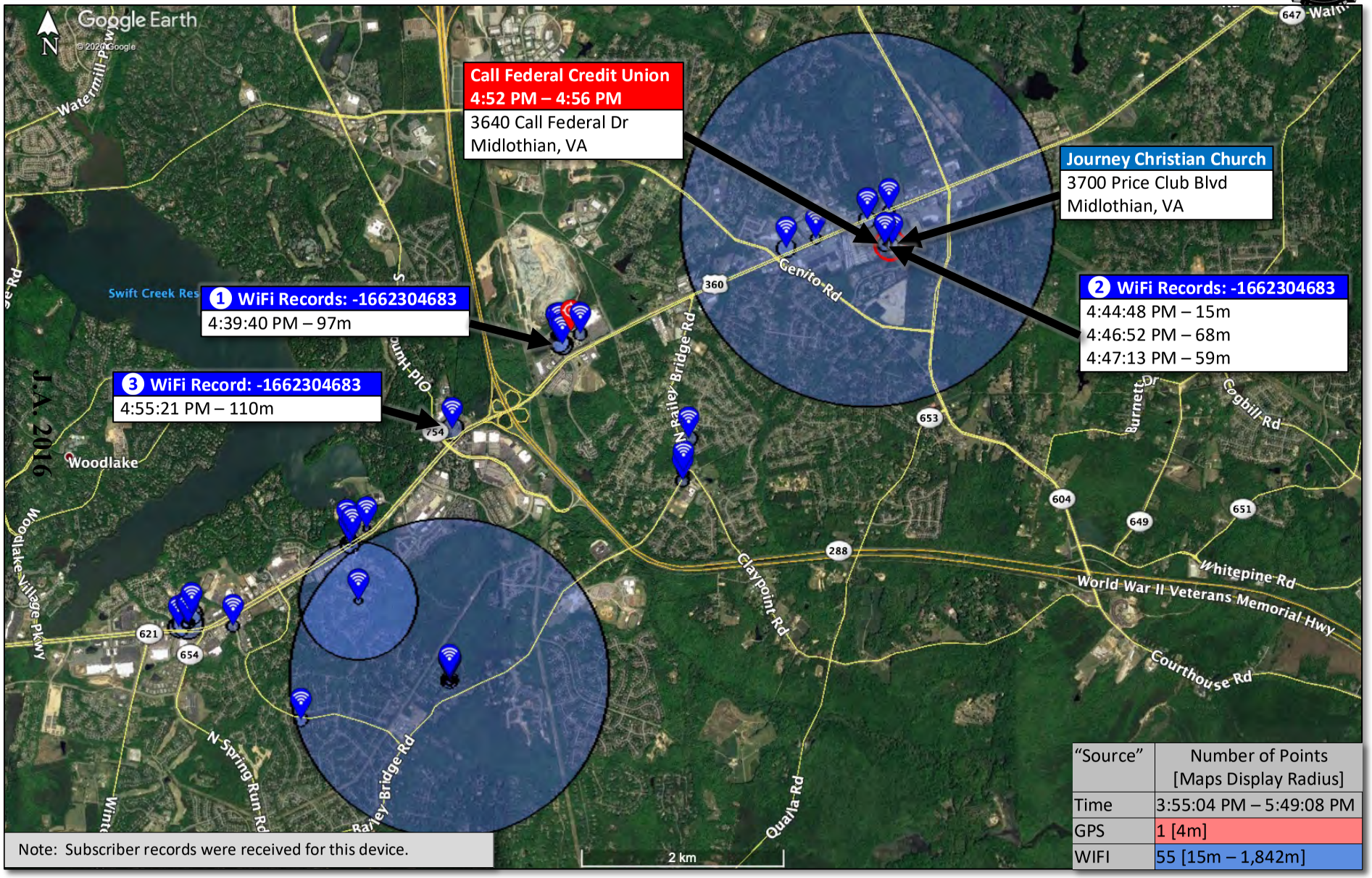
Area of Call Federal Credit Union – May 20, 2019 4:20 PM – 5:20 PM
Initial Google Geofence Records for Device ID -1662304683



Note: Additional records were received for this device.

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Area of Call Federal Credit Union – May 20, 2019 3:50 PM – 5:50 PM
Supplemental Google Geofence Records for Device ID -1662304683



"Source"	Number of Points [Maps Display Radius]
Time	3:55:04 PM – 5:49:08 PM
GPS	1 [4m]
WIFI	55 [15m – 1,842m]

Note: Subscriber records were received for this device.

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM



Samsung Galaxy S9+

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Samsung Galaxy S9+



Features

- Dual Aperture camera
- Super Slow-mo video
- AR Emoji
- Dual Camera
- Infinity Display
- Premium stereo speakers tuned by AKG
- Virtual surround sound by Dolby Atmos
- Stunning colors
- Intelligent Scan – Face Recognition and Iris Scan
- Fingerprint Sensor
- Smart Switch data transfer
- Trade Up Program

Released on March 16, 2018

Source: Samsung – *Galaxy S9 | S9+ Digital Brochure"* and Samsung Newsroom – *"Samsung Electronics Officially Launches Galaxy S9 and S9+"*

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Background of Google, Inc.

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

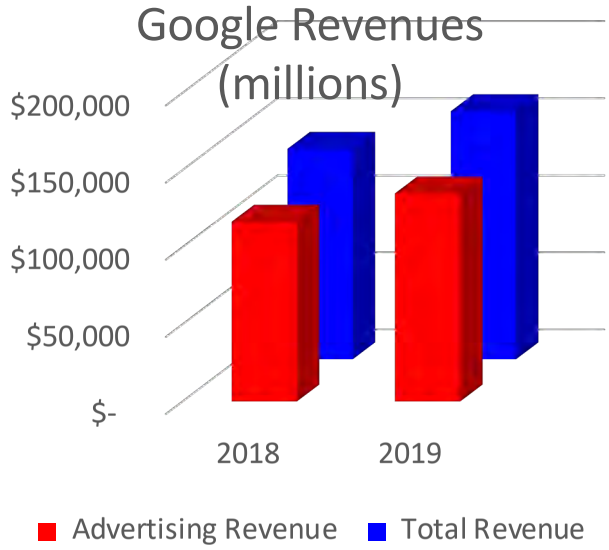
Google

- Google, Inc. (Google) is a subsidiary of Alphabet Inc. (Alphabet), of which Google makes up 99.4% of Alphabet's revenues.
- Alphabet is ranked 11th in the 2020 Fortune 500 index of US companies by revenues with $161,857M.[1]
- "[Alphabet] generate revenues primarily by delivering relevant, cost-effective online advertising." [2]

Period	Google Revenues (millions)	Google Advertising Revenues (millions)	Advertising Revenues as % of Google Revenues
2018	$136,362	$ 116,461	85.4%
2019	$160,743	$ 134,811	83.9%

J.A. 2020

- Google main products include:
  - Ads
  - Android
  - Chrome
  - Hardware
  - Google Cloud
  - Google Maps
  - Google Play
  - Search
  - YouTube



[1]Fortune 500 as of June 17, 2020. [2]Alphabet Inc. Form 10-K dated 2020-02-04. Source: Alphabet Inc. Form 10-K dated 2020-02-04 and Fortune.

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Google Ads – Target Geographic Locations

Target ads to geographic locations

Google Ads location targeting allows your ads to appear in the geographic locations that you choose: countries, areas within a country, a radius around a location, or location groups, which can include places of interest, your business locations, or tiered demographics.

Location targeting helps you focus your advertising on the areas where you'll find the right customers, and restrict it in areas where you won't. This specific type of targeting could help increase your **return on investment (ROI)** as a result.

When it comes to advertising on Google Ads, consider the real estate adage: "Location, location, location!" Regardless of how great your ad is, it probably won't perform as well if it doesn't appear in the right places. Reach your customers where they are and where your business can serve them by using Google Ads location targeting. You can set and then adjust your location targeting settings at any time.

J.A. 2021

Location target	Description	Types of businesses that could benefit	Types of businesses that might not benefit
Radius around a location	Radius targeting (also known as proximity targeting or "Target a radius") allows you to choose to show your ads to customers within a certain distance from your business, rather than choosing individual cities, regions, or countries.	• A business that delivers within a selected radius • A local business whose customer base is within a radius around the business	A business that only wants to reach specific cities, regions, or countries.

Source: Google Ads Help – "*Target Ads to Geographic Locations*"

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Google Ads – Measure Results – Store Visit Conversions

About store visit conversions

If visits to your physical locations—like hotels, auto dealerships, restaurants, and retail stores—are important to your business, you can use conversion tracking to help you see how your ad clicks and viewable impressions influence store visits.

Benefits

- See which campaigns, keywords, and devices drive the most store visits to your business
- Understand your return on investment (ROI) and make more informed decisions about your ad creatives, spend, bid strategies, and other elements of your campaigns
- Evaluate and optimize omnichannel performance by including store visit conversions in your Smart Bidding strategies. Learn more about Smart Bidding for store visits.

How it works

Store visit data is based on anonymous, aggregated statistics. Google Ads creates modeled numbers by using current and past data on the number of people who click or view your ads and later visit your store.

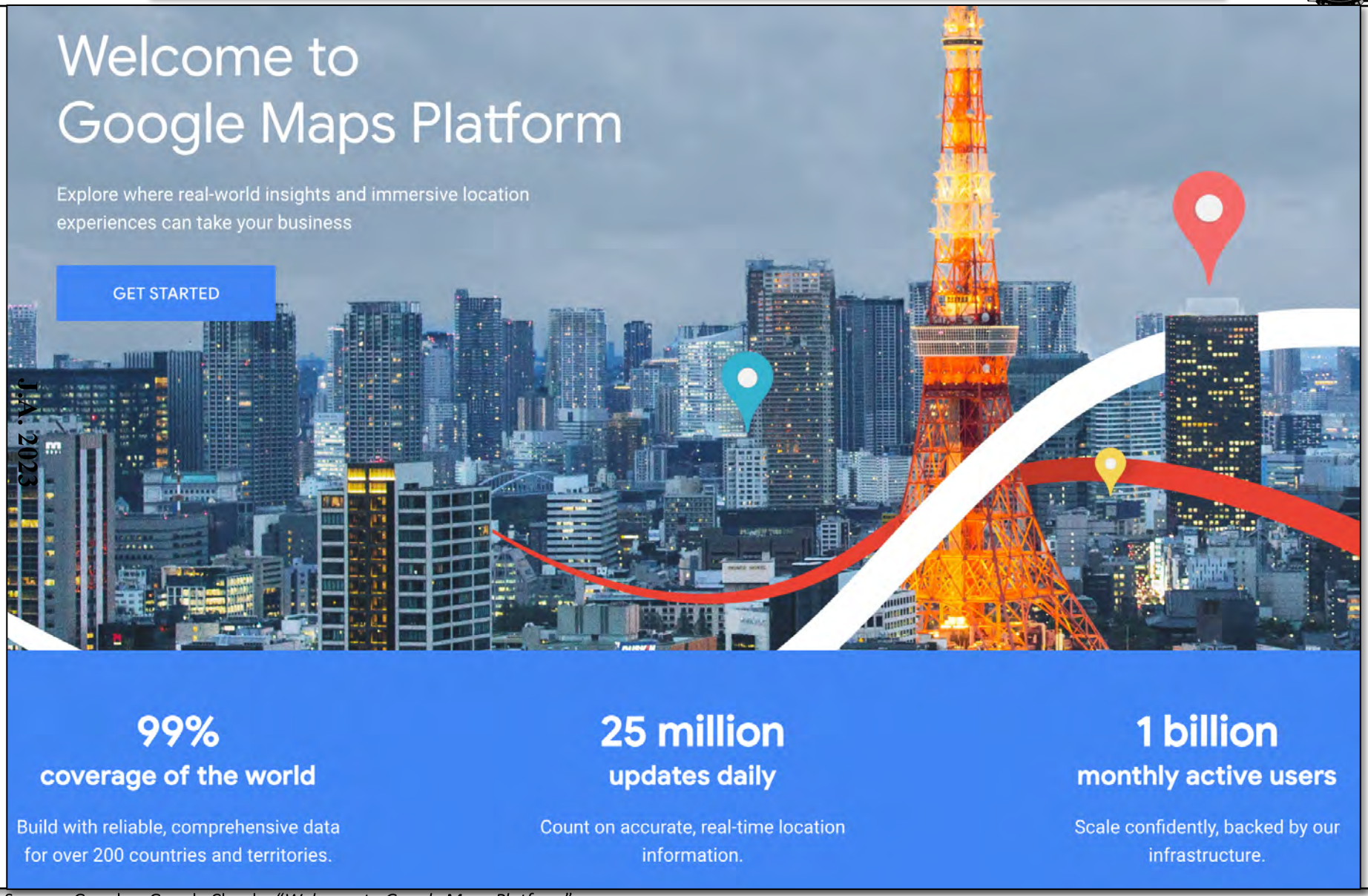
Store visit data can't be tied to individual ad clicks, viewable impressions, or people. We use industry best practices to ensure the privacy of individual users.

J.A. 2022

Source: Google – Google Ads Help – *"About Store Visit Conversions"*

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Google Maps Enterprise Platform



J.A. 2023

Source: Google – Google Cloud – "*Welcome to Google Maps Platform*"

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Google Maps Enterprise Platform – Routes and Places

Places

Help users discover the world with rich details for over 150 million points of interest

GET STARTED

Provide better services with precise location intelligence

Avoid missed pickups by sending your drivers to precise addresses based on users' reported location. Make it easier for users to enter correct billing and shipping information by automatically suggesting addresses as they type. When you use our powerful geolocation and geocoding features in combination with up-to-date Places data, you can get your users the information they need, right when they need it.

Autocomplete

Automatically return location suggestions while users type.

Geocoding

Convert addresses to geographic coordinates, or the reverse.

Geolocation

Return the precise location of a device based on Wi-Fi or cell towers.

J.A. 2024

Routes

Help your users find the best way to get from A to Z with comprehensive data and real-time traffic

GET STARTED

Keep your workforce moving, even during rush hour

Choose faster routes or reallocate deliveries to workers based on real-time traffic conditions. Use predictive traffic models to plan ahead, keeping your workers out of slowdowns and decreasing late deliveries.

Source: Google – Google Cloud – Google Maps Platform – Products – "Places" and "Routes"

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Consumer Services

- Navigation with real-time traffic information

  To get easy, turn-by-turn navigation to places, use the Google Maps app. Maps will show you directions and use real-time traffic information to find the best route to your destination.

- Location-based search

  When you search on Google, we use your location to help show the most relevant search results. For example, if you're in Seattle, when you search for `coffee shops`, you'll see ones that are nearby.

- Location-based ads

  Google's ad products may receive or infer information about your location from a variety of sources. For example, we may use the IP address to identify your general location; we may receive precise location from your mobile device; we may infer your location from your search queries; and websites or apps that you use may send information about your location to us. Google uses location information in our ads products to infer demographic information, to improve the relevance of the ads you see, to measure ad performance and to report aggregate statistics to advertisers.

- Calendar Events – When to leave

  In Google Calendar you can add events, like dinner reservations or birthday parties. In Google Maps, you'll sometimes get notifications about when to leave to get to your event on time.

- Popular Times and Wait Times at Business Locations

  To help customers plan visits to your business, Google may show information including popular times, live visit information, wait times, and typical visit duration. This data appears below your regular business information on Google Maps and Search and can help customers plan their visit.

J.A. 2025

Source: Google – Google Maps Help, Google Search Help, Google Privacy & Terms, and Google My Business Help

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Use of Location Services and Location History

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Google Location Services: On vs. Off

J.A. 2027

When Location is on

- Apps can get your phone's location to give you location-based info or services. Learn how to change app location settings.
- Google Location Services can collect data to improve location-based services. Learn about Google Location Services.
- You can get search results and ads based on your phone's location.
- You can see where your phone is if you lose it. Learn about Find My Device.
- You can share your phone's location with others. Learn about Location Sharing with Google Maps and sending location in emergencies.
- If you have Location History turned on, the places your phone goes will be saved. You can see and manage them later. Learn about Location History.

When Location is off

- Your phone's location isn't shared with any apps. Features that use location may not work properly.
- Google Location Services won't collect data to improve location-based services.
- You can get search results and ads based on your IP address.
- You can't see where your phone is if you lose it. Learn about Find My Device.
- You can't share your phone's location with anyone via Google Maps. Your device can still send it to first responders in an emergency. Learn about Location Sharing with Google Maps and sending location in emergencies.
- Even if you have Location History turned on, the places your phone goes won't be saved. Learn about Location History.

Source: Google – Android Help – "Manage your Android Device's Location Settings"

Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

Google Location History: On vs. Off

When Location History is on

- Google only receives Location History for each device where you are signed in and you have Location Reporting turned on.
- You can change the Location Reporting setting for each device where you're signed in, and limit which devices provide location data to be included in Location History. If you want to change your Location History settings, you can choose to:
  - Report your location from only some of your devices, but not others.
  - Report your location from all your devices.
  - Turn off Location History for your Google Account. Your location won't be reported from any of your devices and you will not have new Location History recorded to your account.
- Your settings for other location services on your device, like Google Location Services and Find My Device, are not changed.

When Location History is off

- New location information is no longer saved to your Location History.
- Previous activity is not deleted from your Location History. You can manually delete your Location History.
- Your settings for other location services on your device, like Google Location Services and Find My Device, are not changed.
- Some location data may continue to be saved in other settings, like Web & App Activity, as part of your use of other services, like Search and Maps, even after you turn off Location History.

Source: Google – Google Account Help – "Manage you Location History"

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM



End of Report

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

End Notes

- Slide 3 – *Determining Location with GPS*
  - GPS.Gov, "How GPS Works." https://www.gps.gov/multimedia/poster/poster-web.pdf. Retrieved February 1, 2020.
  - United States Patent and Trademark Office, United States Patent Number US 9,838,837 B2, "Power-Efficient Location Estimation." https://pimg-fpiw.uspto.gov/fdd/37/388/098/0.pdf. Retrieved on February 3, 2020.
- Slide 4 – *Determining Location with WiFi*
  - United States Patent and Trademark Office, United States Patent Number US 8,339,316 B1, "Smart GPS Use." https://pimg-fpiw.uspto.gov/fdd/16/393/083/0.pdf. Retrieved on Feb 3, 2020.
  - United States Patent and Trademark Office, United States Patent Number US 10,219,103, "Power-Efficient Location Estimation." https://pimg-fpiw.uspto.gov/fdd/03/191/102/0.pdf. Retrieved on February 3, 2020.
- Slide 5 – *WiFi Fingerprinting*
  - Li, Binghao & Quader, Ishrat & Dempster, Andrew. (2008). On outdoor positioning with Wi-Fi. Journal of Global Positioning Systems. 7. 18-26. 10.5081/jgps.7.1.18.
- Slide 6 – *Finding Wireless Access Points*
  - Google, Google Maps Help: "Control Access Point Inclusion in Google's Location Services." https://support.google.com/maps/answer/1725632?hl=en. Retrieved January 29, 2020.
  - Google, Google Privacy & Terms: "How Google Uses Location Information." https://policies.google.com/technologies/location-data. Retrieved January 27, 2020.
- Slide 16 – *Google – Types of Accounts*
  - Google, Android Enterprise Help: *"Types of Google Accounts."* https://support.google.com/work/android/answer/6371476. Retrieved June 13, 2020.
- Slide 38 – *Samsung Galaxy S9+*
  - Samsung, "Galaxy S9 | S9+ Digital Brochure." https://images.samsung.com/is/content/samsung/p5/sg/smartphones/galaxy-s9/Galaxy_S9_Brochure.pdf. Retrieved February 3, 2020.
  - Samsung, Samsung Newsroom: "Samsung Electronics Officially Launches Galaxy S9 and S9+." https://news.samsung.com/global/samsung-electronics-officially-launches-galaxy-s9-and-s9-plus. Retrieved on June 14, 2020.
- Slide 40 – *Google*
  - Fortune – Fortune 500: *"Alphabet."* https://fortune.com/company/alphabet/fortune500/. Retrieved June 17, 2020.
  - Alphabet, "Form 10-K" *dated February 4, 2020*. https://abc.xyz/investor/static/pdf/20200204_alphabet_10K.pdf. Retrieved June 13, 2020.

 Intellectual property of the FBI Cellular Analysis Survey Team. Reproduction in whole or in part is prohibited.

End Notes

- Slide 41 – *Google Ads – Target Geographic Locations*
  - Google, Google Ads Help – "Target Ads to Geographic Locations." https://support.google.com/google-ads/answer/1722043?hl=en&ref_topic=3119074. Retrieved January 29, 2020.
- Slide 42 – *Google Ads – Measure Results – Store Visit Conversions*
  - Google, Google Ads Help - "About Store Visit Conversions." https://support.google.com/google-ads/answer/6100636?hl=en. Retrieved January 31, 2020.
- Slide 43 – *Google Maps Enterprise Platform*
  - Google, Google Cloud – "Welcome to Google Maps Platform." https://cloud.google.com/maps-platform/. Retrieved January 29, 2020.
- Slide 44 – *Google Maps Enterprise Platform – Routes and Places*
  - Google, Google Cloud – Google Maps Platform – "Places." https://cloud.google.com/maps-platform/places/. Retrieved January 29, 2020.
  - Google, Google Cloud – Google Maps Platform – "Routes." https://cloud.google.com/maps-platform/routes/. Retrieved February 1, 2020.
- Slide 45 – *Consumer Services*
  - Google, Google Maps Help – "Use Navigation in the Google Maps App." https://support.google.com/maps/answer/3273406?co=GENIE.Platform%3DiOS&hl=en. Retrieved January 31, 2020.
  - Google, Google Search Help – "Update your Location on Google." https://support.google.com/websearch/answer/179386?co=GENIE.Platform%3DDesktop&hl=en. January 31, 2020.
  - Google, Google Privacy & Terms – "Advertising." https://policies.google.com/technologies/ads. Retrieved January 31, 2020.
  - Google, Google Maps Help – "Turn Google Maps notifications on or off." https://support.google.com/maps/answer/6395563?hl=en. Retrieved January 31, 2020.
  - Google, Google My Business Help – "Popular Times, Wait Times, and Visit Duration." https://support.google.com/business/answer/6263531?hl=en. Retrieved January 31, 2020.
- Slide 47 – *Google Location Services: On vs. Off*
  - Google, Android Help – "Manage your Android Device's Location Settings." https://support.google.com/android/answer/3467281?hl=en. Retrieved January 27, 2020.
- Slide 48 – *Google Location History: On vs. Off*
  - Google, Google Account Help – "Manage Your Location History." https://support.google.com/accounts/answer/3118687?hl=en. Retrieved January 29, 2020.

J.A. 2031

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

GOVERNMENT EXHIBIT
3b
3:19CR130

UNITED STATES OF AMERICA

v.

OKELLO T. CHATRIE,

Defendant.

Case No. 3:19-cr-00130-MHL

SUPPLEMENTAL DECLARATION OF MARLO MCGRIFF

I, Marlo McGriff, respectfully submit this declaration in regard to the above-captioned matter to supplement my prior declaration, filed on March 11, 2020. ECF No. 96-1. I make this declaration based on my knowledge of the facts stated herein.

1. I reviewed the testimony of Spencer McInvaille, Mr. Chatrie's advisory witness, ECF No. 81 ("McInvaille Testimony"), and the video exhibit Mr. McInvaille presented as Exhibit 4 during the January 21, 2020 hearing as to Mr. Chatrie's Motion for Discovery Regarding the Government's Use of Google's Sensorvault Data ("McInvaille Video").

2. As explained in my prior declaration, enabling the Location History ("LH") service requires a Google user to take multiple steps. ECF No. 96-1 at 2.

3. One of those steps, as referenced at ECF No. 96-1 at Paragraph 9, is that the user must opt in to LH in her account settings. LH is disabled in account settings by default, and LH remains disabled unless and until the user enables it.

4. Until recently, a user could enable LH in her account settings during account creation, which can occur during device setup. An example of this is depicted in the McInvaille

Video (at 2:50-3:17) and the McInvaille Testimony (at 50-52). During his testimony, Mr. McInvaille did not enable LH during account creation. *See* McInvaille Testimony at 51-52, 53.

5. A user may also enable LH in her account settings through an app that has LH-powered features, such as the Google Maps app. An example of this is partially depicted in the McInvaille Video (at 4:38-4:45) and the McInvaille Testimony (at 55-57). During his testimony, Mr. McInvaille opened the Google Maps app and was shown a screen stating "Get the most from Google Maps" with two choices: "YES, I'M IN" or "SKIP" as depicted in the last screen at the end of the McInvaille Video (at 4:45); *see* McInvaille Testimony at 56-57.

6. The McInvaille Video ended at that step, without depicting what would happen if the user tapped on "YES, I'M IN." McInvaille Video at 4:45 (stopping at the "Get the most out of Google Maps" screen).

7. By 2017 at the latest, it was not possible for a user to enable LH solely by tapping on "YES, I'M IN" as depicted on the final screen in the McInvaille Video. Instead, a user who tapped on "YES, I'M IN" when prompted would be presented with a second opt-in screen. Only by opting in via that second screen could the user successfully enable LH for her account. Sensorvault rejects LH opt-ins from unsupported flows or devices. Accordingly, Sensorvault would have rejected any attempted opt-in through the manner described by Mr. McInvaille, and LH would not have been successfully enabled.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 12th day of June 2020, in San Francisco.

Marlo McGriff

GOVERNMENT EXHIBIT
4
3:19CR130

From: lers@google.com
Sent: Thursday, June 20, 2019 11:21 AM
To: Hylton, Joshua
Subject: LERS Submission Confirmation - Google Reference. No. 2590472

This is an automated response to advise you that Google Legal Investigations Support has successfully received your legal request submission.

Google receives a very high volume of legal process every day. The team processes legal requests in the order that we receive them. You may monitor the status of your request by logging into your LERS account.

If your request relates to exigent circumstances or if you have further questions, please email USLawEnforcement@google.com and include the Google reference number listed in the subject line. Please include a description of the exigency or your question(s) so that we may assess your request accordingly.

Regards,
Google Legal Investigations Support

From: Hylton, Joshua [redacted]
Sent: Tuesday, June 25, 2019 3:00 PM
To: USLawEnforcement@google.com
Subject: 2590472

Expedition request based on armed and dangerous subject(s) still at large. Subject was on cell phone just prior to violent act; therefore, Google may have captured pertinent information to identify and arrest parties involved.

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: lers@google.com
To: Hylton, Joshua
Subject: Production For Google Reference Number 2590472 Is Available for Download
Date: Friday, June 28, 2019 6:01:43 PM

Your production -- Google Reference Number 2590472 -- is now available for download. Please visit LERS and click on the files link to view all available files.

The download links will expire in 14 days. If you are unable to download your production within this window, contact USLawEnforcement@google.com with your Google Reference Number and we will reinstate the files so long as we still maintain a copy of the files.

If you have questions about your production, please contact USLawEnforcement@google.com with your Google Reference Number in the subject line.

Regards,
Google Legal Investigations Support

From: Hylton, Joshua [redacted]
Sent: Monday, July 01, 2019 4:40 PM
To: USLawEnforcement@google.com
Cc: Simon, Kenneth (USAVAE)
Subject: Google Ref. No. 2590472

Google Legal Team,

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua [redacted]
Sent: Tuesday, July 02, 2019 9:54 AM
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua [redacted]
Sent: Monday, July 08, 2019 9:33 AM
To: USLawEnforcement@google.com
Subject: 2590472

Importance: High

Google Legal Team,

I'm writing to inquire about my correspondence with your office on 07/01 and 07/02. Please keep in mind that expedition is requested based on armed and dangerous subject(s) still being at large. Subject was on cell phone just prior to violent act; therefore, Google may have captured pertinent information to identify and arrest parties involved. See below:

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936

Criminal Investigations Division: Persons Unit

[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua [redacted]
Sent: Tuesday, July 09, 2019 10:37 AM
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

As discussed yesterday over the phone, I appreciate your quick response and willingness to provide GPS data for the below device ID(s). Please expedite this request where possible due to this suspect's continued threat to our community. If it would speed up the process, please provide data as it becomes accessible/available, starting with device ID(s) 1 – 9. It was mentioned that the larger the request, the more time it will take to get data back. With this in mind, I will still have to rule out device ID(s) 1-9; however, I may be able to do so more quickly if I can begin reviewing data. The faster I can review the data, the faster I can get this guy/guys off the street.

Thanks again for your professionalism and understanding. I realize that I'm asking for a lot and you and your team are likely tasked-out already, but any and all assistance and expedited process is MUCH appreciated.

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: lers@google.com
Sent: Tuesday, July 09, 2019 10:25 PM
To: Hylton, Joshua
Subject: Production For Google Reference Number 2590472 Is Available for Download

Your production -- Google Reference Number 2590472 -- is now available for download. Please visit LERS and click on the files link to view all available files.

The download links will expire in 14 days. If you are unable to download your production within this window, contact USLawEnforcement@google.com with your Google Reference Number and we will reinstate the files so long as we still maintain a copy of the files.

If you have questions about your production, please contact USLawEnforcement@google.com with your Google Reference Number in the subject line.

Regards,
Google Legal Investigations Support

From: Hylton, Joshua [redacted]
Sent: Wednesday, July 10, 2019 1:40 PM
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

Thank you guys for the extremely quick turnaround on the Stage Two data. After plotting the nine device ID(s) with additional geographical data, I have narrowed my search for subscriber info to three device ID(s):

1.) **1716665659**
2.) 907512662
3.) -1662304683

Please send me the subscriber information for the above device ID(s) as soon as possible. The involved offender is still a threat to the community and may be a flight risk as well. Again, I can't thank the Google Legal team enough for your professionalism, quick response, and understanding in the captioned matter.

If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua [redacted]
Sent: Thursday, July 11, 2019 9:24 AM
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

Thank you guys for the extremely quick turnaround on Stage(s) One and Two. I'm emailing to inquire about yesterday's request (07/10) for the below device ID(s)' subscriber information. The United States Attorney's Office is waiting for that return before moving forward with additional search warrants.

1.) **1716665659**
2.) 907512662
3.) -1662304683

Please send me what you can as soon as possible. The involved offender is still a threat to the community and is a likely flight risk. Again, I can't thank the Google Legal team enough for your professionalism, quick response, and understanding in the captioned matter.

If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: lers@google.com
Sent: Thursday, July 11, 2019 7:21 PM
To: Hylton, Joshua
Subject: Production For Google Reference Number 2590472 Is Available for Download

Your production -- Google Reference Number 2590472 -- is now available for download. Please visit LERS and click on the files link to view all available files.

The download links will expire in 14 days. If you are unable to download your production within this window, contact USLawEnforcement@google.com with your Google Reference Number and we will reinstate the files so long as we still maintain a copy of the files.

If you have questions about your production, please contact USLawEnforcement@google.com with your Google Reference Number in the subject line.

Regards,
Google Legal Investigations Support

From: Hylton, Joshua [redacted]
Sent: Friday, July 12, 2019 11:37 AM
To: USLawEnforcement@google.com
Cc: Simon, Kenneth (USAVAE)
Subject: 2590472

Google Legal Team,

Thank you guys for getting back with me regarding the subscriber information included with my Stage Three returns. While reviewing data for all three accounts, I could not locate any associated telephone numbers for the following Google account and ID:

- Okellochatrie55@gmail.com
- Google Account ID: 365520819283

Please include any such data, as the following is listed in my search warrant:

"After review and upon request by Law Enforceemnt, Google Inc. shall provide identifying account information/CSI for the accounts requested by Law Enforcement. This identifying account information/CSI **shall include all of the following that are available:** user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account**, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used t set up the account, verify the account or to receive assistance with the account, and Google Voice phone numbers associated with the account."**

Please let me know what you find, as soon as possible, as the offender involved is still a threat to the community and may be a flight risk as well. I will CC Assistant United States Attorney, Kenneth Simon, for tracking purposes or follow-up questions.

If you have any concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 246 of 288 Total Pages:(2112 of 2164)

GOVERNMENT EXHIBIT 5 3:19CR130

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

Effective January 22, 2019 | Archived versions | Download PDF

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for key terms. And if you have any questions about this Privacy Policy, you can contact us.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 247 of 288 Total Pages:(2113 of 2164)

INFORMATION GOOGLE COLLECTS

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

Things you create or provide to us

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 248 of 287 Total Pages:(2114 of 2164)

Information we collect as you use our services

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 249 of 288 Total Pages:(2115 of 2164)

- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

You can visit your Google Account to find and manage activity information that's saved in your account.

Go to Google Account

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- IP address
- Sensor data from your device
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 250 of 288 Total Pages:(2116 of 2164)

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

WHY GOOGLE COLLECTS DATA

We use data to build better services

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 251 of 288 Total Pages:(2117 of 2164)

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, Security Checkup provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.

Go to Ad Settings

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 252 of 288 Total Pages:(2118 of 2164)

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 253 of 287 Total Pages:(2119 of 2164)

For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

YOUR PRIVACY CONTROLS

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the Privacy Checkup, which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our Product Privacy Guide.

Go to Privacy Checkup

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 254 of 287 Total Pages:(2120 of 2164)

We also built a place for you to review and control information saved in your Google Account. Your Google Account includes:

Privacy controls

Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.

Go to Activity Controls

Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

Go to Ad Settings

About you

Control what others see about you across Google services.

Go to About You

Shared endorsements

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 255 of 288 Total Pages:(2121 of 2164)

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

Go to Shared Endorsements

Information you share

Control whom you share information with through your account on Google+.

Go to Information You Share

Ways to review & update your information

My Activity

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

Go to My Activity

Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

Go to Dashboard

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 256 of 287 Total Pages:(2122 of 2164)

Your personal information

Manage your contact information, such as your name, email, and phone number.

Go to Personal Info

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: Choose whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your YouTube Search History and your YouTube Watch History.
- Ad Settings: Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

You can also request to remove content from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from specific Google services

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 257 of 288 Total Pages:(2123 of 2164)

- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

And finally, Inactive Account Manager allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a cookie in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services rely on cookies to function properly, for things like remembering your language preferences.
- Device-level settings: Your device may have controls that determine what information we collect. For example, you can modify location settings on your Android device.

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 258 of 288 Total Pages:(2124 of 2164)

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing a song in Play, your name and photo appear next to your activity. We may also display this information in ads depending on your Shared endorsements setting.

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you use Google Home to make a reservation through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We'll ask for your explicit consent to share any sensitive personal information.

With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite), your domain administrator and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 259 of 287 Total Pages:(2125 of 2164)

- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our Transparency Report.
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 260 of 288 Total Pages:(2126 of 2164)

advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

KEEPING YOUR INFORMATION SECURE

We build security into our services to protect your information

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like Safe Browsing, Security Checkup, and 2 Step Verification to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

EXPORTING & DELETING YOUR INFORMATION

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 261 of 288 Total Pages:(2127 of 2164)

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

In some cases, we retain data for limited periods when it needs to be kept for legitimate business or legal purposes. You can read about Google's data retention periods, including how long it takes us to delete your information.

We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 262 of 287 Total Pages:(2128 of 2164)

Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

ABOUT THIS POLICY

When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

Changes to this policy

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 263 of 288 Total Pages:(2129 of 2164)

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to archived versions for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

RELATED PRIVACY PRACTICES

Specific Google services

The following privacy notices provide additional information about some Google services:

- Chrome & the Chrome Operating System
- Play Books
- Payments
- Fiber
- Google Fi
- G Suite for Education
- YouTube Kids
- Google Accounts Managed with Family Link, for Children under 13 (or applicable age in your country)

Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 264 of 288 Total Pages:(2130 of 2164)

- Your Google Account is home to many of the settings you can use to manage your account
- Privacy Checkup guides you through key privacy settings for your Google Account
- Google's safety center helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
- Privacy & Terms provides more context regarding this Privacy Policy and our Terms of Service
- Technologies includes more information about:
  - How Google uses cookies
  - Technologies used for Advertising
  - How Google uses pattern recognition to recognize things like faces in photos
  - How Google uses information from sites or apps that use our services

ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." Learn more about Google ads and why you may see particular ads.

the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you contact most frequently.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 265 of 287 Total Pages:(2131 of 2164)

phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. Learn more

payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. Learn more

devices

For example, we can use information from your devices to help you decide which device you'd like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 266 of 287 Total Pages:(2132 of 2164)

like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features.

Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. Learn more

services to make and receive calls or send and receive messages

Examples of these services include:

- Google Hangouts, for making domestic and international calls
- Google Voice, for making calls, sending text messages, and managing voicemail
- Google Fi, for a phone plan

Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 267 of 288 Total Pages:(2133 of 2164)

Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. Learn more

publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate.

protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

deliver our services

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 268 of 287 Total Pages:(2134 of 2164)

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account
- Photos and videos you upload to Google Photos are used to help you create albums, animations, and other creations that you can share. Learn more
- A flight confirmation email you receive may be used to create a “check-in” button that appears in your Gmail
- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it’s taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 269 of 288 Total Pages:(2135 of 2164)

customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can learn more here. You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can search and browse privately or turn off signed-out search personalization.

personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. Learn more

sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services.

may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. Learn more

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 270 of 288 Total Pages:(2136 of 2164)

safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.
- The “last account activity” feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. Learn more

detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

combine the information we collect

Some examples of how we combine the information we collect include:

- When you’re signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. Learn more

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 271 of 288 Total Pages:(2137 of 2164)

- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. Learn more

- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based your activity. Learn more

- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. Learn more

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

Learn more about how Google uses data when you use our partners' sites or apps.

partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. Learn more

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 272 of 288 Total Pages:(2138 of 2164)

specific Google services

For example, you can delete your blog from Blogger or a Google Site you own from Google Sites. You can also delete reviews you've left on apps, games, and other content in the Play Store.

rely on cookies to function properly

For example, we use a cookie called 'lbcs' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. Learn more

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our Transparency Report.

show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. Learn more

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 273 of 288 Total Pages:(2139 of 2164)

specific partners

For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. Learn more about these partners and how they use your information.

servers around the world

For example, we operate data centers located around the world to help keep our products continuously available for users.

third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

appropriate safeguards

For example, we may anonymize data, or encrypt data to ensure it can't be linked to other information about you. Learn more

ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 274 of 288 Total Pages:(2140 of 2164)

Customizing our services

For example, we may display a Google Doodle on the Search homepage to celebrate an event specific to your country.

Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. Learn more about the companies providing business services in the EU.

Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 275 of 288 Total Pages:(2141 of 2164)

Cookies and similar technologies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.

Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

Pixel tag

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 276 of 288 Total Pages:(2142 of 2164)

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These “server logs” typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for “cars” looks like this:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 -
740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user’s ISP. Depending on the user’s service, a different address may be

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 277 of 288 Total Pages:(2143 of 2164)

assigned to the user by their service provider each time they connect to the Internet.

- `25/Mar/2003 10:15:32` is the date and time of the query.
- `http://www.google.com/search?q=cars` is the requested URL, including the search query.
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used.
- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

Unique identifiers

A unique identifier is a string of characters that can be used to uniquely identify a browser, app, or device. Different identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed.

Unique identifiers can be used for various purposes, including security and fraud detection, syncing services such as your email inbox, remembering your preferences, and providing personalized advertising. For example, unique identifiers stored in cookies help sites display content in your browser in your preferred language. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. Learn more about how Google uses cookies.

On other platforms besides browsers, unique identifiers are used to recognize a specific device or app on that device. For example, a unique identifier such as the Advertising ID is used to provide relevant advertising on Android devices, and can be managed in your device's settings. Unique identifiers may also be incorporated into a device by its manufacturer (sometimes called a universally unique ID or UUID), such as the IMEI-number of a mobile phone. For example, a device's unique identifier can

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 278 of 287 Total Pages:(2144 of 2164)

be used to customize our service to your device or analyze device issues related to our services.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 279 of 287 Total Pages:(2145 of 2164)

GOVERNMENT EXHIBIT
5a
3:19CR130

GOOGLE TERMS OF SERVICE

Last modified: October 25, 2017 (view archived versions)

Welcome to Google!

Thanks for using our products and services ("Services"). The Services are provided by Google LLC ("Google"), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.

By using our Services, you are agreeing to these terms. Please read them carefully.

Our Services are very diverse, so sometimes additional terms or product requirements (including age requirements) may apply. Additional terms will be available with the relevant Services, and those additional terms become part of your agreement with us if you use those Services.

Using our Services

You must follow any policies made available to you within the Services.

Don't misuse our Services. For example, don't interfere with our Services or try to access them using a method other than the interface and the instructions that we provide. You may use our Services only as permitted by law, including applicable export and re-export control laws and regulations. We may suspend or stop providing our Services to you if you do not comply with our terms or policies or if we are investigating suspected misconduct.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 280 of 288 Total Pages:(2146 of 2164)

Using our Services does not give you ownership of any intellectual property rights in our Services or the content you access. You may not use content from our Services unless you obtain permission from its owner or are otherwise permitted by law. These terms do not grant you the right to use any branding or logos used in our Services. Don't remove, obscure, or alter any legal notices displayed in or along with our Services.

Our Services display some content that is not Google's. This content is the sole responsibility of the entity that makes it available. We may review content to determine whether it is illegal or violates our policies, and we may remove or refuse to display content that we reasonably believe violates our policies or the law. But that does not necessarily mean that we review content, so please don't assume that we do.

In connection with your use of the Services, we may send you service announcements, administrative messages, and other information. You may opt out of some of those communications.

Some of our Services are available on mobile devices. Do not use such Services in a way that distracts you and prevents you from obeying traffic or safety laws.

Your Google Account

You may need a Google Account in order to use some of our Services. You may create your own Google Account, or your Google Account may be assigned to you by an administrator, such as your employer or educational institution. If you are using a Google Account assigned to you by an administrator, different or additional terms may apply and your administrator may be able to access or disable your account.

To protect your Google Account, keep your password confidential. You are responsible for the activity that happens on or through your Google Account. Try not to reuse your Google Account password on third-party applications. If you learn of any unauthorized use of your password or Google Account, follow these instructions.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 281 of 287 Total Pages:(2147 of 2164)

Privacy and Copyright Protection

Google's privacy policies explain how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policies.

We respond to notices of alleged copyright infringement and terminate accounts of repeat infringers according to the process set out in the U.S. Digital Millennium Copyright Act.

We provide information to help copyright holders manage their intellectual property online. If you think somebody is violating your copyrights and want to notify us, you can find information about submitting notices and Google's policy about responding to notices in our Help Center.

Your Content in our Services

Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.

When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service. Also, in some of our Services, there are terms or settings that narrow the scope of our use of the content submitted

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 282 of 287 Total Pages:(2148 of 2164)

in those Services. Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.

If you have a Google Account, we may display your Profile name, Profile photo, and actions you take on Google or on third-party applications connected to your Google Account (such as +1's, reviews you write and comments you post) in our Services, including displaying in ads and other commercial contexts. We will respect the choices you make to limit sharing or visibility settings in your Google Account. For example, you can choose your settings so your name and photo do not appear in an ad.

You can find more information about how Google uses and stores content in the privacy policy or additional terms for particular Services. If you submit feedback or suggestions about our Services, we may use your feedback or suggestions without obligation to you.

About Software in our Services

When a Service requires or includes downloadable software, this software may update automatically on your device once a new version or feature is available. Some Services may let you adjust your automatic update settings.

Google gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software provided to you by Google as part of the Services. This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Google, in the manner permitted by these terms. You may not copy, modify, distribute, sell, or lease any part of our Services or included software, nor may you reverse engineer or attempt to extract the source code of that software, unless laws prohibit those restrictions or you have our written permission.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 283 of 287 Total Pages:(2149 of 2164)

Open source software is important to us. Some software used in our Services may be offered under an open source license that we will make available to you. There may be provisions in the open source license that expressly override some of these terms.

Modifying and Terminating our Services

We are constantly changing and improving our Services. We may add or remove functionalities or features, and we may suspend or stop a Service altogether.

You can stop using our Services at any time, although we'll be sorry to see you go. Google may also stop providing Services to you, or add or create new limits to our Services at any time.

We believe that you own your data and preserving your access to such data is important. If we discontinue a Service, where reasonably possible, we will give you reasonable advance notice and a chance to get information out of that Service.

Our Warranties and Disclaimers

We provide our Services using a commercially reasonable level of skill and care and we hope that you will enjoy using them. But there are certain things that we don't promise about our Services.

OTHER THAN AS EXPRESSLY SET OUT IN THESE TERMS OR ADDITIONAL TERMS, NEITHER GOOGLE NOR ITS SUPPLIERS OR DISTRIBUTORS MAKE ANY SPECIFIC PROMISES ABOUT THE SERVICES. FOR EXAMPLE, WE DON'T MAKE ANY COMMITMENTS ABOUT THE CONTENT WITHIN THE SERVICES, THE SPECIFIC FUNCTIONS OF THE SERVICES, OR THEIR RELIABILITY, AVAILABILITY, OR ABILITY TO MEET YOUR NEEDS. WE PROVIDE THE SERVICES "AS IS".

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 284 of 287 Total Pages:(2150 of 2164)

SOME JURISDICTIONS PROVIDE FOR CERTAIN WARRANTIES, LIKE THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. TO THE EXTENT PERMITTED BY LAW, WE EXCLUDE ALL WARRANTIES.

Liability for our Services

WHEN PERMITTED BY LAW, GOOGLE, AND GOOGLE'S SUPPLIERS AND DISTRIBUTORS, WILL NOT BE RESPONSIBLE FOR LOST PROFITS, REVENUES, OR DATA, FINANCIAL LOSSES OR INDIRECT, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES.

TO THE EXTENT PERMITTED BY LAW, THE TOTAL LIABILITY OF GOOGLE, AND ITS SUPPLIERS AND DISTRIBUTORS, FOR ANY CLAIMS UNDER THESE TERMS, INCLUDING FOR ANY IMPLIED WARRANTIES, IS LIMITED TO THE AMOUNT YOU PAID US TO USE THE SERVICES (OR, IF WE CHOOSE, TO SUPPLYING YOU THE SERVICES AGAIN).

IN ALL CASES, GOOGLE, AND ITS SUPPLIERS AND DISTRIBUTORS, WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE THAT IS NOT REASONABLY FORESEEABLE.

Business uses of our Services

If you are using our Services on behalf of a business, that business accepts these terms. It will hold harmless and indemnify Google and its affiliates, officers, agents, and employees from any claim, suit or action arising from or related to the use of the Services or violation of these terms, including any liability or expense arising from claims, losses, damages, suits, judgments, litigation costs and attorneys' fees.

USCA4 Appeal: 22-4489 Doc: 19-8 Filed: 01/20/2023 Pg: 285 of 287 Total Pages:(2151 of 2164)

About these Terms

We may modify these terms or any additional terms that apply to a Service to, for example, reflect changes to the law or changes to our Services. You should look at the terms regularly. We'll post notice of modifications to these terms on this page. We'll post notice of modified additional terms in the applicable Service. Changes will not apply retroactively and will become effective no sooner than fourteen days after they are posted. However, changes addressing new functions for a Service or changes made for legal reasons will be effective immediately. If you do not agree to the modified terms for a Service, you should discontinue your use of that Service.

If there is a conflict between these terms and the additional terms, the additional terms will control for that conflict.

These terms control the relationship between Google and you. They do not create any third party beneficiary rights.

If you do not comply with these terms, and we don't take action right away, this doesn't mean that we are giving up any rights that we may have (such as taking action in the future).

If it turns out that a particular term is not enforceable, this will not affect any other terms.

The laws of California, U.S.A., excluding California's conflict of laws rules, will apply to any disputes arising out of or relating to these terms or the Services. All claims arising out of or relating to these terms or the Services will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.

For information about how to contact Google, please visit our contact page.

GOVERNMENT EXHIBIT
6
3:19CR130

CURRICULUM VITAE

Jeremy A. D'Errico
Federal Bureau of Investigation
Richmond Division
1970 East Parham Road
Richmond, Virginia 23228
Telephone: (804) 261-1044

PROFESSIONAL EXPERIENCE

Special Agent (October 2014 – Present)
Federal Bureau of Investigation
Richmond, Virginia

Special Agent D'Errico is currently assigned to the Violent Crime and Transnational Organized Crime squad where he investigates computer-enabled organized crime, threat-to-life matters, and provides assistance for federal, state and local investigations. Special Agent D'Errico was previously assigned to the Cyber squad where he investigated computer intrusion and criminal matters involving computers.

Cellular Analysis Survey Team (CAST) (May 2016 – Present)
Special Agent D'Errico responsibilities include:

- Analysis of historical call detail records for homicide investigations, fugitive investigation, child abductions, and other violent crimes; and
- Preparation of numerous historical cell site analyses and maps for various federal, state and local law enforcement agencies.

Computer Scientist (September 2012 – October 2014)
Federal Bureau of Investigation
Richmond, Virginia

Computer Scientist D'Errico's responsibilities included:

- Investigating high priority criminal and national security matters using sophisticated technical methods and analysis;
- Liaising with strategic partners and develop relationships within the community in support of investigations and intelligence collection;
- Developing technical solutions to accelerate the investigative process; and
- Interpreting technical results and data for the investigative team.

Lead Information System Engineer (February 2006 – September 2012)
The MITRE Corporation
Richmond, Virginia

Mr. D'Errico's responsibilities included managing and leading a work program that provided advanced technical support, tools, and expertise on computer intrusion investigations.

Intern (June 2005 – November 2005)
Federal Bureau of Investigation
Richmond, Virginia

Mr. D'Errico's responsibilities included developing an investigative data solution for analyzing disparate sets of case-specific data.

PROFESSIONAL EXPERIENCE (Continued)

Consultant (August 2000 – October 2005)
CGI-AMS
Richmond, Virginia

Mr. D'Errico responsibilities included leading the development, testing and deployment of computer telephony integration (CTI) applications for customer call center.

EDUCATION

Johns Hopkins University - Baltimore, Maryland
Master of Security Informatics (MSSI), 2005.

James Madison University – Harrisonburg, Virginia
Graduate courses in Information Security, 2004.

James Madison University - Harrisonburg, Virginia
Bachelor of Science (BS), Computer Science, 2000.

PROFESSIONAL TRAINING

- Cellular Analysis Survey Team (CAST) Re-certification (Feb 2020)
- Cellular Analysis Survey Team (CAST) Re-certification (Feb 2019)
- Cellular Analysis Survey Team (CAST) Certification, Part II (Sept 2018)
- Cellular Analysis Survey Team (CAST) Certification, Part I (Aug 2018)
- Cellular Analysis Survey Team (CAST) Field Training Exercise (FTX) (Jun 2018)
- Cellular Analysis Survey Team (CAST) Advanced Training (Apr 2018)
- Joint Child Abduction Rapid Deployment Team Training (Nov 2017)
- SANS Advanced Smartphone Forensics (Nov 2017)
- Cellular Analysis Survey Team (CAST) Basic Training (May 2016)
- Various training courses in computer forensics and information security from October 2009 to present

CERTIFICATIONS

- FBI – Cellular Analysis Survey Team (CAST)
- FBI – Digital Extraction Technician (DExT)
- FBI – Computer Analysis Response Team (CART) Technician
- Guidance Software – EnCase Certified Examiner (EnCE)
- ISC^2 – Certified Information Systems Security Professional (CISSP)
- Global Information Assurance Certification – Open Source Intelligence (GOSI)
- Global Information Assurance Certification – Certified Forensic Analyst (GCFA)
- Global Information Assurance Certification – Reverse Engineering Malware (GREM)
- Global Information Assurance Certification – Certified Incident Handler (GCIH)
- Global Information Assurance Certification – Advanced Smartphone Forensics (GASF)
- Global Information Assurance Certification – Security Essentials (GSEC)

INSTRUCTION

- Prosecuting Homicide Cases – Historical Cell Site and Geolocation Data (Nov 2020)
- Cyber-Attacks, Internet Investigations, Forensic Analysis & Electronic Records (CIIFER) – Historical Cell Site and Geolocation Data (Mar 2020)
- Advanced Homicide/Violent Crimes Investigations – Social Media / Location History (Mar 2020)
- Basic Historical Cell Site Analysis (Feb 2020)
- Advanced Homicide/Violent Crimes Investigations – Social Media / Location History (Jun 2019)
- Basic Historical Cell Site Analysis (May 2019)
- Advanced Homicide/Violent Crimes Investigations – Social Media / Location History (May 2019)
- Advanced Homicide/Violent Crimes Investigations – Social Media / Location History (Mar 2019)
- Advanced Homicide/Violent Crimes Investigations – Social Media / Location History (Nov 2018)
- Central Shenandoah Criminal Justice Training Academy – Social Media (Apr 2018)
- Southwest Virginia Criminal Justice Training Academy – Social Media (May 2017)
- Crater Criminal Justice Training Academy – Social Media (May 2017)
- Rappahannock Regional Criminal Justice Academy – Social Media (Mar 2017)
- Japan National Police Force – Virtual Currency Investigation (Aug 2016)
- Central Shenandoah Criminal Justice Training Academy – Cyber Intrusions (Aug 2016)
- Cardinal Justice Academy – Crimes Against Children (Jul 2015)
- Southwest Virginia Criminal Justice Training Academy – Social Media (May 2015)
- FBI Computer Scientist Field Operations Training Class 14-02 (Jul 2014)
- FBI Computer Scientist Field Operations Training Class 14-01 (Apr 2014)
- Crater Criminal Justice Training Academy – Cyber Intrusions (Mar 2014)
- FBI Computer Scientist Field Operations Training Class 13-01 (Sep 2013)

RECOGNITION

- US Attorney's Office, Eastern District of VA – Law Enforcement Public Service Award (2020, 2014, 2009, 2008)

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Richmond Division (The Hon. M. Hannah Lauck)

JOINT APPENDIX

VOLUME 9 of 11 (pages 2091 - 2092)

JESSICA D. ABER
United States Attorney

Kenneth R. Simon, Jr., Ass't U.S. Attorney
Peter S. Duffey, Ass't U.S. Attorney
Counsel for Appellee
919 East Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400

Nathan P. Judish, Senior Counsel
Computer Crime & Intel. Property Section
Criminal Division
U.S. Department of Justice

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
Counsel for Appellant
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800

Michael W. Price, Litigation Dir.
NACDL Fourth Amendment Ctr.
1660 L Street NW, 12th Floor
Washington, DC 20036

This page intentionally left blank for double-sided pagination and printing

TABLE OF CONTENTS

VOLUME 1 (pages 1 - 176)

District Court Docket Sheet (as of Jan. 17, 2023) 1

Indictment (Sept. 17, 2019, Doc. 1) 22

Defendant's Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Oct. 29, 2019, Doc. 29) 25

Government's Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (Nov. 19, 2019, Doc. 41) 51

Defendant's Reply to Government's Response [to] Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (Dec. 9, 2019, Doc. 48) 76

Exh. A (First Step 2 Request to Google) (Doc. 48-1) 98
Exh. B (Second Step 2 Request to Google) (Doc. 48-2) 100
Exh. C (Third Step 2 Request to Google) (Doc. 48-3) 102
Exh. D (Transcript, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019)) (Doc. 48-4) ..... omitted from J.A.

Government's Notice Regarding Attachment of Google Geofence State Search Warrant to Response in Opposition to Motion to Suppress (Dec. 18, 2019, Doc. 54) 104

Affidavit for search warrant and warrant, with attachments (Doc. 54-1) 107

Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant (Dec. 20, 2019, Doc. 59-1) 118

United States' Response to Amicus Curiae Brief of Google LLC (Jan. 10, 2020, Doc. 71) 148

Defendant's Response to Google's Motion to File Amicus Curiae Brief in Support of Neither Party (Jan. 10, 2020, Doc. 72) 158

VOLUME 2 (pages 177 - 416)

Transcript, Discovery Motion Hearing (Jan. 21, 2020, Doc. 81; *see* Doc. 77 (court minutes))....177

Preliminary matters....179

Def't witness Spencer McInvaille — Direct examination....193; Cross examination....283; Redirect examination....306

Argument by the defense....318
Argument by the government....332
Rebuttal by the defense....350

Court's ruling....355

Defendant's Supplemental Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (May 22, 2020, Doc. 104)....363

United States' Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (June 12, 2020, Doc. 109)....393

VOLUME 3 (pages 417 - 694)

Transcript, Suppression Motion Hearing, Day 1 (evidence) (Mar. 4, 2021, Doc. 201; *see* Doc. 198 (court minutes))....417

Preliminary matters....420

Def't witness Spencer McInvaille — Direct examination....432; Cross examination....542; Redirect examination....586

Def't witness Marlo McGriff — Direct examination....606

VOLUME 4 (pages 695 - 1070)

Transcript, Suppression Motion Hearing, Day 2 (evidence) (Mar. 5, 2021, Doc. 202; *see* Doc. 199 (court minutes)) 695

Preliminary matters 698

Def't witness Marlo McGriff, cont'd — Direct examination ..... 699; Cross examination ..... 791; Redirect examination 841

Def't witness Sarah Rodriguez — Direct examination ..... 862; Cross examination ..... 902; Redirect examination 916

Gov't witness Jeremy D'Errico — Direct examination ..... 923; Cross examination ..... 967; Redirect examination 1010

Gov't witness Joshua Hylton — Direct examination ..... 1016; Cross examination ..... 1040; Redirect examination 1063

Concluding matters 1064

VOLUME 5 (pages 1071 - 1326)

Defendant's Post-Hearing Brief on "Geofence" General Warrant (May 3, 2021, Doc. 205) 1071

Government's Response in Opposition to Defendant's Motion for Suppression (May 21, 2020, Doc. 214; *see* Doc. 207-2) 1117

Defendant's Reply to Government's Response in Opposition to Motion for Suppression (June 4, 2020, Doc. 213) 1164

Transcript, Suppression Hearing (arguments) (June 24, 2021, Doc. 217; *see* Doc. 215 (court minutes)) 1185

Argument by the defense 1187
Argument by the government 1231
Rebuttal by the defense 1313

Concluding matters 1322

VOLUME 6 (pages 1327 - 1456)

Memorandum Opinion (denying suppression motion) (Mar. 3, 2022, Doc. 220) 1327

Order (denying suppression motion) (Mar. 3, 2022, Doc. 221) 1390

Criminal Information (May 6, 2022, Doc. 224) 1391

Transcript, Change of Plea Hearing (May 9, 2022, Doc. 247; *see* Doc. 226) 1394

Plea Agreement (May 9, 2022, Doc. 228) 1428

Statement of Facts (May 9, 2022, Doc. 229) 1444

Judgment in a Criminal Case (Aug. 19, 2022, Doc. 239) 1449

Notice of Appeal (Aug. 25, 2022, Doc. 241) 1456

VOLUME 7 (pages 1457 - 1810) – DOCUMENT EXHIBITS

Exhibits Admitted at Discovery Motion Hearing (Jan. 21, 2020)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) ..... *see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) ..... *see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) ..... *see* J.A. 2093
Def't Exh. 4: Activation Video ..... omitted from J.A., available on request
Def't Exh. 5: Three Paths Video (sealed) ..... *see* J.A. 2139
Def't Exh. 6: First Step 2 Request to Google 1457
Def't Exh. 7: Second Step 2 Request to Google 1459
Def't Exh. 8: Third Step 2 Request to Google 1461

Def't Exh. 9: Step 3 Request to Google 1463

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header) .....*see* J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1) .....*see* J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed) .....*see* J.A. 2093
Def't Exh. 5: Three Paths Video (sealed) .....*see* J.A. 2139
Def't Exh. 6: Spencer McInvaille Report 1464
Def't Exh. 7: Spencer McInvaille Supplemental Report 1469
Def't Exh. 8: CSV Google Data File (.csv file) .....*see* J.A. 2139
Def't Exh. 9: Unique in Crowd Study 1475
Def't Exh. 11: September 2018 Oracle Submission 1480
Def't Exh. 18: Federal Search Warrant Application & Attachments 1502
Def't Exh. 19: State Search Warrants & Attachments 1534
Def't Exh. 21: McGriff Declaration 1 (Doc. 96-1) 1551
Def't Exh. 23: McGriff Declaration 3 (Doc. 147) 1562
Def't Exh. 24: Rodriguez Declaration (Doc. 96-2) 1579
Def't Exh. 27: Every Step You Take 1587
Def't Exh. 30: AZ Ex. 18 (admitted portions only) 1631
Def't Exh. 31: AZ Ex. 19 (admitted portions only) 1633
Def't Exh. 32: AZ Ex. 20 1639
Def't Exh. 33: AZ Ex. 24 1644
Def't Exh. 34: AZ Ex. 202 1667
Def't Exh. 36: AZ Ex. 209 1777
Def't Exh. 38: AZ Ex. 219 1781
Def't Exh. 40: AZ Ex. 236 1797
Def't Exh. 41: AZ Ex. 260 1804

VOLUME 8 (pages 1811 - 2090) – DOCUMENT EXHIBITS, CONT'D

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021), cont'd

Def't Exh. 43: May 2018 Privacy Policy – Redline 1811
Def't Exh. 43a: May 2018 Privacy Policy – Redline (with internet source information) 1840
Def't Exh. 44: Jan. 2019 Privacy Policy – Redline 1865
Def't Exh. 45: Oct. 2019 Privacy Policy – Redline 1895
Def't Exh. 46: McGriff Blog 1 1926

Def't Exh. 47: McGriff Blog 2 1929
Def't Exh. 48: 2018 Quartz Article 1934
Def't Exh. 49: 2018 AP Article 1 1941
Def't Exh. 51: 2019 NYT Article 1948
Def't Exh. 53: Blumenthal-Markey Letter to FTC 1957

Gov't Exh. 1: CAST PowerPoint Presentation 1981
Gov't Exh. 2: Geofence Warrant (Doc. 54-1) ..... *see* J.A. 107
Gov't Exh. 3: Declaration of Marlo McGriff (Mar. 11, 2020)
(same as Def't Exh. 21 (Doc. 96-1)) ..... *see* J.A. 1551
Gov't Exh. 3a: Declaration of Sarah Rodriguez (Mar. 11, 2020)
(same as Def't Exh. 24 (Doc. 96-2)) ..... *see* J.A. 1579
Gov't Exh. 3b: Supplemental Declaration of McGriff (June 17, 2020)
(Doc. 110-1) 2032
Gov't Exh. 3c: Third Declaration of Marlo McGriff (Aug. 7, 2020)
(same as Def't Exh. 23 (Doc. 147)) ..... *see* J.A. 1562
Gov't Exh. 4: Joshua Hylton emails with Google 2034
Gov't Exh. 5: Google Privacy Policy 2048
Gov't Exh. 5a: Google Terms of Service 2081
Gov't Exh. 6: Special Agent D'Errico's C.V. 2088
Gov't Exh. 12: "Got to Be Mobile" Video ..... *see* J.A. 2091

VOLUME 9 (pages 2091 - 2092) – DIGITAL MEDIA EXHIBIT

Gov't Exh. 12: "Got to Be Mobile" Video (admitted only at suppression motion hearing) ..... (.mp4 file)

VOLUME 10 (pages 2093 - 2138) – SEALED DOCUMENT EXHIBIT

Def't Exh. 3: PDF of Raw Data (*see* Doc. 69 (sealing order)) (admitted at both discovery motion hearing and suppression motion hearing) 2093

VOLUME 11 (pages 2139 - end) – SEALED DIGITAL MEDIA EXHIBITS

Def't Exh. 5: Three Paths Video (admitted at both discovery motion hearing and suppression motion hearing) ..... (.mp4 file)
Def't Exh. 8: CSV Google Data File (admitted only at suppression motion hearing) ..... (.csv file, viewable in Excel)

Gov't Exh. 12 ("Got to Be Mobile" Video)
(file name: 22-4489 Chatrie Govt Exh 12.mp4)

This file has been scanned for viruses and found to be virus-free.

This page intentionally left blank for double-sided pagination and printing