IN THE
UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 22-4489

UNITED STATES OF AMERICA,

Appellee,

v.

OKELLO T. CHATRIE,

Appellant.

Appeal from the United States District Court
for the Eastern District of Virginia at Richmond
The Honorable M. Hannah Lauck, District Judge

BRIEF OF THE UNITED STATES

Jessica D. Aber
United States Attorney
Eastern District of Virginia

Kenneth A. Polite, Jr.
Assistant Attorney General

Richard W. Downing
Deputy Assistant Attorney General

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Eastern District of Virginia

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
United States Department of Justice
1301 New York Ave., NW
Washington, DC 20530
(202) 616-7203

Attorneys for the United States of America

Table of Contents

Table of Authorities

Introduction

Defendant Okello Chatrie robbed a bank at gunpoint near Richmond, Virginia, and got away with nearly $200,000. He carried a cell phone with him, and investigators later identified him as the robber using a Google geofence warrant: a warrant requiring Google to disclose its records of location information for cellular devices present at a specified place and time. This investigative technique supplies investigators with a new source of crime-scene evidence comparable to traditional video surveillance tapes.

Based on an affidavit that stated that the robber possessed a cellular phone during the robbery and that explained why it was likely that Google would have information regarding that phone's location, a Virginia magistrate found probable cause to believe that Google possessed evidence of the robbery, and he issued a geofence search warrant. The warrant authorized the government to obtain from Google two hours of location information associated with electronic devices that were within 150 meters of the site of the bank robbery during a one-hour interval containing the robbery. This circle included both the bank and nearby parking areas; it avoided major roads.

The warrant required the government to follow a three-step process. First, the warrant directed Google to disclose to the government location coordinates (but not identity information) for devices present in the targeted area within the hour of

the robbery. Second, the warrant directed law enforcement to attempt to narrow down devices of interest by comparing the location coordinates Google produced with the facts of the robbery, and it directed Google to disclose location coordinates for the resulting set of devices during a two-hour period that encompassed the robbery. Third, the warrant directed that law enforcement use this additional information to further attempt to narrow down the devices of interest, and it directed Google to disclose identifying information for those devices. Pursuant to the warrant, Google produced one hour of location information for 19 devices, two hours of location information for nine, and identity information for three. From this information, investigators identified Defendant and solved the robbery.

The district court denied Defendant's motion to suppress the information that the government obtained pursuant to the geofence warrant, and Defendant ultimately pleaded guilty to two robbery-related counts, reserving his right to appeal the district court's denial of his suppression motion. This Court should affirm the district court's decision for three independent reasons: (1) Defendant had no protected Fourth Amendment interest in the geofence information; (2) the geofence warrant satisfied the Fourth Amendment's requirements for search warrants; and (3) officers relied in good faith on the warrant.

Statement of Jurisdiction

Defendant appeals from a judgment of conviction in a criminal case. The district court had jurisdiction under 18 U.S.C. § 3231 and entered judgment on August 19, 2022. JA1449. Defendant filed a timely notice of appeal on August 25, 2022. JA1456; *see* Fed. R. App. P. 4(b)(1)(A)(i). This Court has jurisdiction to review the judgment of conviction under 28 U.S.C. § 1291.

Issue Presented

Whether the district court correctly declined to suppress information that Google disclosed to the government pursuant to a geofence warrant that authorized disclosure of location and identity information associated with cellular devices present at the site of an armed bank robbery.

Statement of the Case

In 2019, a grand jury in the Eastern District of Virginia issued a two-count indictment charging defendant with forced accompaniment during an armed credit union robbery, in violation of 18 U.S.C. §§ 2113(a), 2113(d), and 2113(e), and 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)(i) and (ii). JA22-JA24. The counts were based on Defendant's robbery of the Call Federal Credit Union in Midlothian, Virginia. JA22.

Defendant filed a motion to suppress evidence that Google disclosed to the government pursuant to a geofence warrant, JA1071-JA1116, and the district court denied the motion. JA1327-JA1390. Defendant pleaded guilty to a two-count information; the plea preserved his right to appeal the denial of the geofence suppression motion. JA1391-JA1393; JA1428-JA1448. Defendant was convicted of armed credit union robbery, in violation of 18 U.S.C. §§ 2113(a) and 2113(d), and using, carrying, and brandishing a firearm in relation to a crime of violence, in violation of 18 U.S.C. §§ 924(c)(1)(A)(i) and (ii). JA1449. The court sentenced Defendant to 141 months' imprisonment and 3 years' supervised release. JA1450-JA1451.

A. Defendant robbed the Call Federal Credit Union.

At approximately 4:50 pm on May 20, 2019, Defendant entered the Call

Federal Credit Union in Midlothian, Virginia. JA112, JA1025, JA1444. He held a cell phone to his face and appeared to be speaking to someone. JA112, JA1025. 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." JA112.

After the teller replied that she did not have access to that amount of money, Defendant pulled out a firearm. JA112, JA1026. He forced everyone to the ground at gunpoint and escorted the manager and others to the vault in the back. JA112, JA1026. He forced the manager to open the safe and place $195,000 into a bag. JA112. He then fled. JA112; JA1026-JA1027.

B. The magistrate issued a geofence warrant for specified location information associated with the robbery of the Call Federal Credit Union.

Following the robbery, Federal Bureau of Investigation Task Force Officer ("TFO") Josh Hylton responded to the scene to investigate. JA1024. Because the robber had carried a phone, TFO Hylton knew that there was a possibility that the robber might have worked with others, such as a lookout or a driver. JA112, JA1027. He also knew that Google could have information that would show the robber's phone was in the area at the time of the robbery. JA112-JA113, JA1027. On three prior occasions, after consulting with prosecutors, TFO Hylton had obtained geofence warrants directed to Google. JA1020-JA1021. A geofence

warrant requires Google to disclose information about Google users whose Location History indicates their devices were in a specified area during a specified time. JA1558.

On June 14, 2019, TFO Hylton sought and obtained a geofence warrant from the Chesterfield Circuit Court of Virginia. JA107-JA117. His statement of probable cause began by describing the facts of the robbery, including that before the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone. JA112. The statement then explained why there was reason to believe that Google would have evidence pertaining to the robbery. JA113. Among other facts, the statement disclosed that: (1) as of 2013, 56% of cell phones were smartphones; (2) "[n]early every" Android phone "has an associated Google account"; (3) Google "collects and retains location data" from such devices when the account owner enables Google location services; and (4) Google collects location information from non-Android smartphones if the devices are "registered to a Google account and the user has location services enabled." JA113. Magistrate David Bishop issued the geofence warrant upon a finding of probable cause. JA114.

The geofence warrant specified a geographical area, identified as a circle of radius 150 meters around a specific latitude and longitude point near the bank. JA117. It covered the bank and nearby parking areas, some of which belonged to a

nearby church that also fell within the geofence, and it went up to but did not reach major roads. JA117. 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). JA116, JA117. The warrant also authorized disclosure of specified customer identity information associated with these accounts, including usernames and email addresses. JA117.

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. JA116. The warrant directed that in the first step, Google would disclose anonymized location information for devices present in the target area during the hour of the robbery, but not the identity information associated with the devices. JA116. In particular, the warrant directed that Google disclose "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." JA116.

In the second step, the warrant directed law enforcement to review the anonymized location information produced by Google and "attempt to narrow down the list by reviewing the time-stamped location coordinates for each account and comparing that information against the known time and location" of the

robbery. JA116. After law enforcement provided the updated list to Google, the warrant directed that Google then 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. JA116-JA117. In the third step, the warrant directed that law enforcement again attempt to narrow down the accounts that remained of interest, and that Google disclose username and other specified subscriber identity information for those accounts. JA117.

Investigators followed this three-step process in executing the warrant. JA950-JA967. In the first step, Google provided 209 data points concerning 19 accounts (including 36 points from Defendant's account), all within the 150-meter circle and during the hour of the bank robbery. JA951-JA952, JA2000, JA2002, JA2098-JA2104. For each data point, Google produced a device ID, date and time, latitude and longitude coordinate, source of information (wi-fi or GPS), and "map display radius." JA1997. "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. JA629, JA1559-JA1560. To identify responsive information, Google ran a computation against all stored Location History coordinates to determine which ones matched the geofence parameters. JA1559.

By reviewing the step 1 data in conjunction with witness interviews and

video surveillance tapes, investigators concluded that Defendant's device likely belonged to the robber. JA966-JA967.

In the second step, TFO Hylton, in consultation with federal prosecutors, initially asked Google for data regarding all 19 accounts, but Google was nonresponsive. JA1039, JA2038. Concerned about the danger that the robber posed to the public, TFO Hylton called Google, and he ultimately narrowed the second-stage production to nine accounts. JA1039, JA2042. Google produced two hours of location data for each of these accounts—a total of 680 data points, including 94 from Defendant's account. JA2006, JA2109-JA2129. This information showed Defendant's presence at the bank and his movement on public roads. JA956-JA960, JA2008.

In the third step, TFO Hylton directed Google to disclose subscriber information for three accounts, including the account of Defendant. JA960, JA2134-JA2137. This information included Defendant's email address. JA961.

C. Defendant opted in to Google storage of his Location History and agreed Google could use his information in accordance with its privacy policies.

Google Location History allows users "to keep track of locations they have visited while in possession of their compatible mobile devices." JA1552-JA1553. 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." JA764, JA1553.

According to Google Location History Product Manager Marlo McGriff, 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. JA795-JA796, JA1558-JA1559. Google also uses Location History in multiple ways for advertising purposes. JA612-JA614, JA977-JA978, JA1555. It uses "radius targeting," which targets ads to users based on their proximity to a particular business. JA614. It uses location information to measure "store visit conversions"—how many customers who saw a particular ad went on to visit a relevant store. JA612-JA613, JA1555. It infers users' interests from where they visit, and it uses that "semantic location information" to target advertising to users. JA1553, JA1555. A Google user may review, edit, or delete Location History information. JA738, JA805, JA833, JA1556. A Google user may also stop collection of Location History information. JA833.

Google's logs show that on July 9, 2018, Defendant opted in to the Location History service. JA1563, JA1577. Google's Location History service is off by default; a user must explicitly opt in to the service. JA1553. In 2019, approximately one-third of active Google users had Location History enabled.

JA804, JA1555.

Location History Product Manager McGriff declared that on July 9, 2018, a user could not opt in without following Google's "supported consent flow," a term that refers to the "the steps and consent text necessary to opt in" to the Location History service. JA1564, JA793. Under the supported consent flow, 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

JA1564.[1] 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." JA1566, JA713-JA715. Google's logs do not indicate the particular application or opt-in screen Defendant used to opt in to Location History. JA1564.

[1] Along with this text, Google presented an expansion arrow to the user that the user could tap to obtain additional information about Location History. JA1565. Among other information, this expanded Location History text stated: "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." JA1565.

Google records also showed that Defendant created the email account Okellochatrie55@gmail.com on August 20, 2017. JA1562, JA1575. At that time, he agreed to Google's terms of service, which specified that Google could use data "in accordance with [Google's] privacy policies." JA799, JA2083.[2] Google's Privacy Policy in effect on the date of the bank robbery 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.

JA2051-JA2053, JA2056.

D. The district court denied Defendant's motion to suppress.

Defendant filed a motion to suppress the geofence warrant and its fruits. JA1071. He argued that (1) he had a reasonable expectation of privacy in his

[2] The terms of service available at that time are also available at https://policies.google.com/terms/archive/20140414. Location History Product Manager McGriff stated that evidence of Google's privacy policy and terms of service could be found online. JA803.

Location History information; (2) the geofence warrant was an unconstitutional general warrant; and (3) the good faith exception did not apply. JA1089-JA1115. Regarding good faith, Defendant explicitly disclaimed any challenge to the warrant based on *Franks v. Delaware*, 438 U.S. 154 (1978). JA1115.

After multiple rounds of briefing from the United States and Defendant, amicus briefing and affidavits from Google, and an evidentiary hearing,[3] the district court denied Defendant's motion and issued a lengthy opinion. JA1327-JA1389. First, the court stated that because it would deny Defendant's motion on other grounds, it need not resolve whether Defendant had a reasonable expectation of privacy in the geofence data. JA1361. Nevertheless, the court offered some observations on this issue, including its concern that Fourth Amendment doctrine was "lagging behind technological innovations," its observation that "[o]rdinarily, a criminal perpetrator would not have a reasonable expectation of privacy in his or her activities within or outside the publicly accessible bank," and its "skepticism" that the third-party doctrine would apply to geofence information. JA1362-JA1363, JA1378.

[3] Hearing witnesses included defense expert Spencer McInvaille, Google Location History Product Manager Marlo McGriff, Google Team Lead for Legal Investigations Support Sarah Rodriguez, FBI Special Agent Jeremy D'Errico, and TFO Hylton. JA433-JA1064.

Second, the court held that the warrant violated the Fourth Amendment. JA1364-JA1378. Regarding probable cause, the court acknowledged that "a fair probability may have existed that the Geofence Warrant would generate the *suspect*'s location information." JA1369. However, drawing from cases addressing arrest warrants or physical searches of persons, the court found this probability inadequate, and it held that "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."' JA1367. Because the district court believed the warrant could not meet this standard for everyone within the geofence, the court held that it violated the Fourth Amendment. JA1375. The court also held that the warrant was insufficiently particular, concluding that the geofence was too large and that steps 2 and 3 of the warrant left too much discretion to the executing officers. JA1369, JA1376-JA1378.

Finally, the court denied the motion to suppress based on the good-faith exception to the exclusionary rule. *See United States v. Leon*, 468 U.S. 897 (1984); JA1381-JA1388. The court found the warrant neither facially deficient nor so lacking in indicia of probable cause that investigators could not rely on it. JA1381-JA1388. The court explained that its conclusion was bolstered by the fact that geofence warrants were a novel investigative technique, such that no court had yet ruled on their legality when TFO Hylton sought the warrant, and TFO Hylton

had consulted with prosecutors prior to obtaining previous geofence warrants. JA1382-JA1383.

Defendant subsequently entered a conditional guilty plea to two counts, preserving his right to appeal the denial of his geofence suppression motion. JA1428, JA1432. This appeal of the district court's denial of the geofence suppression motion followed.

Summary of Argument

For three separate reasons, this Court should affirm the district court's denial of Defendant's suppression motion. First, Defendant lacked any protected Fourth Amendment privacy interest in the two hours of location information that Google disclosed about his devices. Obtaining short-term location information is not a Fourth Amendment search under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (*en banc*). In addition, Defendant disclosed his location to Google to obtain location-based services, and the United States therefore did not violate the Fourth Amendment when it obtained that information from Google.

Second, the geofence warrant complied with the Fourth Amendment because it was supported by probable cause and sufficiently particular. Regarding probable cause, the affidavit established that a bank had been robbed, that the robber had a cell phone, and that there was a fair probability that Google would store evidence

of the robbery. As to particularity, the warrant was appropriately tailored temporally and geographically to collect evidence related to the robbery: it was limited to two hours of location information for devices that were, over a one-hour interval, within 150 meters of the site of the bank robbery. This circle covered the bank and nearby parking areas, but not major roads.

Third, suppression of evidence in this case is not appropriate because investigators reasonably relied in good faith on the geofence warrant. Suppression is inappropriate under *Leon*: the warrant was not facially deficient or so lacking in probable cause that an investigator could not rely on it. Moreover, when TFO Hylton obtained the geofence warrant in 2019, a geofence warrant was a new investigative technique—there were no judicial opinions analyzing geofence warrants. It was therefore reasonable for an investigator to rely on the warrant after consulting with counsel about geofence warrants, obtaining prior geofence warrants from state judges and a United States Magistrate Judge, and then obtaining the warrant from a magistrate.

Accordingly, this Court should affirm the judgment.

Argument

In order for this Court to reverse the district court, Defendant must prevail on three arguments: that he had a protected Fourth Amendment privacy interest in the information Google disclosed to the United States, that the geofence warrant

violated the Fourth Amendment, and that officers did not rely on the warrant in good faith. He prevails on none.

This Court reviews the district court's factual findings for clear error and its legal conclusions *de novo*, and the evidence must be viewed in the light most favorable to the government, the party that prevailed in the district court. *United States v. Davis*, 690 F.3d 226, 233 (4th Cir. 2012). When a claim is waived, it is not reviewable on appeal. *United States v. Morehouse*, 34 F.4th 381, 395 (4th Cir. 2022).

This Court may affirm "on any grounds apparent from the record." *United States v. Smith*, 395 F.3d 516, 519 (4th Cir. 2005); *see also Greenlaw v. United States*, 554 U.S. 237, 250 n.5 (2008) ("[T]he appellee may, without taking a cross-appeal, urge in support of a decree any matter appearing in the record.") (quoting *United States v. American Railway Express Co.*, 265 U.S. 425, 435 (1924)). Thus, although the district court chose not to determine whether the geofence warrant invaded Defendant's Fourth Amendment interests and held that the warrant violated the Fourth Amendment, this Court may affirm the district court's denial of Defendant's suppression motion either because Defendant had no protected Fourth Amendment interest in the geofence information or because the warrant complied with the Fourth Amendment.

I. Defendant had no protected Fourth Amendment interests in any information disclosed pursuant to the geofence warrant.

The geofence warrant information can be divided into three categories: two hours of Defendant's location information, Defendant's subscriber identity information, and information pertaining to other Google customers. Defendant has not claimed that he had a protected Fourth Amendment interest in the latter two categories, and any such argument would be foreclosed by controlling precedent. *See United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (holding that subscriber had no protected Fourth Amendment interest in subscriber identity information); *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (holding that Fourth Amendment rights "may not be vicariously asserted").

Nor does Defendant have any protected Fourth Amendment interests in the two hours of information Google disclosed about his location. The Supreme Court has explained that the existence of protected Fourth Amendment interests in location information held by a third party lies "at the intersection of two lines of cases": cases addressing "a person's expectation of privacy in his physical location and movements" and cases addressing "what a person keeps to himself and what he shares with others." *Carpenter*, 128 S. Ct. at 2214-16. Here, as discussed below, each of these two lines of cases provides independent reasons to conclude that Google's disclosure of two hours of Defendant's location information did not infringe his Fourth Amendment rights. Defendant bears the

burden of establishing that he has a protected privacy interest in the information he seeks to suppress, *see United States v. Daniels*, 41 F.4th 412, 415 (4th Cir. 2022), and he has not met that burden here.

A. Defendant lacked protected Fourth Amendment interests in two hours of information regarding his location.

In *Carpenter v. United States*, 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 [a phone company's 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 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. In short, *Carpenter* recognized a privacy interest only in certain long-term, comprehensive location information.

Although *Carpenter* declined to resolve whether obtaining less than seven days of cell phone location information constitutes a search, *Carpenter*'s reasoning demonstrates that obtaining two hours of location information does not. The Court framed 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 cited its previous holding from *United States v. Knotts*, 460 U.S. 276, 282 (1983), that a person "on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," *id.* at 2215, but it cautioned that *Knotts* had reserved whether this principle applied to "more sweeping modes of surveillance." *Id.* *Carpenter* 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." *Id.* at 2220. 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 here when it obtained two hours of Defendant's location information pursuant to the geofence warrant.

Leaders of a Beautiful Struggle v. Baltimore Police Department, 2 F.4th 330 (4th Cir. 2021) (*en banc*) (hereinafter "*Leaders*"), confirmed the distinction between long-term and short-term location tracking. In *Leaders*, this Court held that a Baltimore aerial surveillance program, under which the city collected and retained for at least 45 days a "record of where everyone came and went within the city during daylight hours," was a search under *Carpenter*. *Id.* at 341, 346. *Leaders* held that "*Carpenter* solidified the line between short-term tracking of

public movements—akin to what law enforcement could do '[p]rior to the digital age'—and prolonged tracking that can reveal intimate details through habits and patterns." *Id.* at 341. Under *Carpenter*, "[t]he latter form of surveillance invades the reasonable expectation of privacy that individuals have in the whole of their movements and therefore requires a warrant." *Id.* The 45-day surveillance period was not short-term because it exceeded "ordinary police capabilities": "[p]eople understand that they may be filmed by security cameras on city streets, or a police officer could stake out their house and tail them for a time." *Id.* at 345.

Here, the United States obtained only two hours of Defendant's location information. This acquisition is consistent with ordinary police capabilities identified by *Leaders*: security cameras and being tailed. The warrant's step 1 information is similar to security camera footage: it captured Defendant's presence and movement in close proximity to the bank. JA2003. The warrant's step 2 information, which tracked Defendant as he drove on public roads, is similar to the tracking approved by the Supreme Court in *Knotts*. JA2008. Thus, under *Leaders*, the United States did not infringe Defendant's Fourth Amendment interests. Rather than providing an encyclopedic chronicle of Defendant's life, the information disclosed by Google showed his device's location for less than half an afternoon.

Importantly, in assessing whether the government has conducted a search under *Carpenter* and *Leaders*, a court assesses the quantity of information accessed by the government, not the quantity of information possessed by the provider. This Court confirmed this analysis in *Leaders*: "*Carpenter* was clear on that issue: a search took place 'when the Government *accessed CSLI* from the wireless carriers.'" *Leaders*, 2 F.4th at 344 (quoting *Carpenter*, 138 S. Ct. at 2219). The district court expressed concern that Google retains information for each user who opts in, JA1362, but under *Carpenter* and *Leaders*, Google's retention of information about Defendant does not transform the government's acquisition of a small portion of that information into a search.

Finally, other courts have agreed that *Carpenter* protects only comprehensive, long-term location information. In *United States v. Hammond*, 996 F.3d 374, 387-92 (7th Cir. 2021), the Seventh Circuit held that real-time tracking of a specified cell phone over a period of approximately six hours was not a search. In addition, other courts have held that cell tower dumps, which are similar to geofence warrants in that they reveal information about cellular devices present in a specified location at a specified time, are not Fourth Amendment searches. *See, e.g., United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019); *United States v. Walker*, 2020 WL 4065980, at *8 (W.D.N.C. July 20, 2020); *United State v. Rhodes*, 2021 WL 1541050, at *2 (N.D. Ga. Apr. 20, 2021). The

United States did not infringe Defendant's Fourth Amendment interests when it obtained two hours of his location information from Google.

B. Defendant lacked protected Fourth Amendment interests in location information he disclosed to Google to obtain location-based services.

There is a second, independent reason why Defendant had no protected Fourth Amendment interests in the location information Google disclosed to the United States: Defendant voluntarily disclosed information about the location of his phone to Google to obtain location-based services. Thus, Google's disclosure of that information to the government 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 cases ranging from private conversations to business records, the Supreme Court has repeatedly held that the Fourth Amendment does not protect information voluntarily 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 the location information Defendant disclosed to Google to obtain location-based services.

In *Carpenter*, the Supreme Court held that the third-party doctrine did not apply to a phone company's cell phone location information, but the Court did not reject the third-party doctrine or "disturb the application 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 for three reasons: because the phone company collects cell-site information "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." *Id.* at 2220. These three factors are not present for Google's Location History service. First, as the district court found, Location History "is off by default," and a user must opt into storage of Location History. JA1333, JA1553. In fact, Google could not obtain and store Defendant's device 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. JA1554. Second, Defendant also had discretion to delete any or all of his Location History.

JA738, JA833, JA1556.[4] Finally, 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. JA804, JA1555.

Defendant's voluntary disclosure of his phone's location to Google is evident from the nature of the relationship between Google and its users: users must provide their devices' location to Google to obtain location-based services. Courts often infer that an individual 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 consider Miller's explicit agreements with his bank. Instead, the Court determined that Miller disclosed financial information to the bank by "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, in *Smith v. Maryland*, the Court held that "[a]ll telephone users realize that they must 'convey' phone numbers to

[4] The district court noted that an unidentified Google employee once stated in an email that deleting data was difficult, JA1342, but the record demonstrates that Google informed users that they could see and delete their data. JA1564, JA2058-JA2059. Nothing in the record demonstrates that a user who sought to delete his data would be unable to do so.

the telephone company, since it is through telephone company switching equipment that their calls are completed." *Smith*, 442 U.S. at 742. The Ninth Circuit recently applied this analysis to disclosure of location information in *Sanchez v. Los Angeles Dep't of Transportation*, 39 F.4th 548 (9th Cir. 2022), in which the court rejected a Fourth Amendment challenge to a Los Angeles regulation mandating that e-scooter companies disclose to its transportation department real-time location data for every scooter. The court explained that when one "rents an e-scooter, he plainly understands that the e-scooter company must collect location data for the scooter through its smartphone applications. Thus, the voluntary exposure rationale fits far better here than in *Carpenter*." *Id.* at 559.

The same reasoning applies here. Google customers disclose their devices' locations 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. JA764, JA1553. Google also uses location information to target advertisements to users via radius targeting, store visit conversions, and inferences drawn from Location History. JA612-JA614, JA1553, JA1555. These services demonstrate that Google is not merely providing a storage service for users to store their own location information. Based on a user's location, Google provides services that are helpful to the user, to other users, to advertisers, and to

Google itself. In sum, a user of Google's location services does not keep his location private; instead, the user shares location information with Google to obtain location-based services. Thus, the user's Fourth Amendment interests are not infringed when Google discloses his location information to the government.

The opt-in process necessary for Google to store Location History further confirms that Defendant voluntarily disclosed his device's location to Google. Defendant could not have successfully opted in without Google presenting the supported consent flow language to him. JA1564-JA1566.[5] That language informed Defendant that Location History "[s]aves where you go with your devices," that "[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences," and that "[y]ou can see your data, delete it and change your settings at account.google.com." JA1564. This language set forth the core components of Google's Location History service: that Google would store Defendant's location information and that Google would use that information to provide services to Defendant. Defendant then clicked

[5] Location History Product Manager McGriff explained that "[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." JA714.

"TURN ON" in response, thereby agreeing to disclose his location to Google. JA1566.[6]

Finally, Google's Privacy Policy further supports the fact that Defendant voluntarily disclosed his phone's location information to Google. Courts rely on privacy policies in evaluating whether a customer discloses information to a service provider. *See, e.g.*, *Sanchez*, 39 F.4th at 559 (stating that e-scooter user "must agree to the operator's privacy policies," which allow collection and storage of location data). Here, 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." JA2051. The Privacy Policy also stated that: "you can turn on Location History if you want traffic predictions for your daily commute." JA2056. This language confirms that Google users share their location with Google in order for Google to

[6] The district court questioned whether this language was sufficient because it did not detail the frequency with which data would be recorded, the amount of data, or the precision of data. JA1380. But the data that Google saved fell within the scope of what Defendant agreed Google would do: save where he went with his phone. Moreover, the Supreme Court has held that if one discloses information to a third party, the third party's storage decisions lack constitutional significance. *See Smith v. Maryland*, 442 U.S. at 745 (stating that a phone company's choice to store 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").

provide them with location-based services. The United States did not infringe his Fourth Amendment interests when it obtained that information from Google.[7]

II. The geofence warrant complied with the Fourth Amendment.

This Court may affirm the district court's denial of Defendant's suppression motion on the basis that the warrant complied with the Fourth Amendment. A warrant satisfies the Fourth Amendment if it is: (1) supported by probable cause; (2) sufficiently particular; and (3) issued by a neutral and disinterested magistrate. *See Dalia v. United States*, 441 U.S. 238, 255 (1979). Here, the affidavit established a fair probability that Google would have evidence of the robbery, and the warrant described that evidence with mathematical precision.

A. 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

[7] The district court stated that it could not determine whether Defendant voluntarily disclosed his location to Google based on the "murky" record, JA1378, but its analysis focused on the opt-in process for Location History and ignored the nature of the relationship between Google and its users: users provide their device location to Google to obtain location-based services. JA1378-JA1380. In addition, although the exact mechanism through which Defendant opted in to storage of Location History is uncertain, the consent flow language essential to opting in successfully is not. JA1564-JA1566, JA714.

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 provided an ample basis for the issuing magistrate's finding of probable cause. In particular, the affidavit established that: (1) an unknown subject committed an armed bank robbery at a particular place and time; (2) prior to the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone; (3) the majority of cell phones were smartphones; (4) "[n]early every" Android phone "has an associated Google account," and Google "collects and retains location data" from such devices when the account owner enables Google location services; and (5) 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." JA112-JA113. This information gave the magistrate a substantial basis to conclude that there was a fair probability that Google possessed evidence related to the robbery. Indeed, although the district court found that the warrant lacked probable cause as to other users within the geofence, it did conclude that "a fair probability may have existed

that the Geofence Warrant would generate the *suspect's* location information." JA1369.

Moreover, the Supreme Court broadly construes what may constitute evidence for purposes of a search warrant. In *Messerschmidt v. Millender*, 565 U.S. 535, 539 (2012), police obtained a warrant for "all guns and gang-related material" in connection with a known gang member shooting at his ex-girlfriend. The Court provided multiple reasons why "all gang-related materials" could be seized as evidence in connection with someone shooting at his ex-girlfriend, including that the materials could "help to establish motive," could be "helpful in impeaching [the shooter]," could be helpful in "rebutting various defenses," and 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 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, probable cause existed because the information

sought by the warrant was in fact evidence appropriately seized pursuant to a search warrant.

The Supreme Court's decision in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), sets forth the probable cause analysis applicable here. In *Zurcher*, the Supreme Court approved a search warrant that authorized the search of a newspaper's office to seize photographs of a crime scene at which unidentified individuals had assaulted police officers. *See id.* at 551, 553-560. That warrant was analogous to the one here: it authorized seizure, from a third party not suspected of crime, of crime-scene evidence to identify perpetrators and others present at the scene of a crime. The Court held that "[t]he critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." *Id.* at 556. 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.* at 559.

The district court found that the warrant failed to establish "particularized" probable cause, JA1368, but its analysis is inconsistent with the *Zurcher* standard. The court stated that "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.'" JA1367 (citing *Maryland v. Pringle*, 540 U.S. 366, 371 (2003)). But *Pringle* addresses whether probable cause existed for an arrest of a person, not the standard for obtaining a search warrant to search a specified place for evidence of crime. *See Pringle*, 540 U.S. at 374. As the Supreme Court held in *Zurcher*, "[i]n situations where the State does not seek to seize 'persons' but only those 'things' which there is probable cause to believe are located on the place to be searched, there is no apparent basis in the language of the Amendment for also imposing the requirements for a valid arrest—probable cause to believe that the third party is implicated in the crime." *Zurcher*, 436 U.S. at 554.

The district court also cited cases addressing physical searches of persons pursuant to warrants to search premises, including *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. JA1367. But *Ybarra* and its progeny explicitly address limitations on physical searches of persons pursuant to warrants, not the standard for searching property (such as the information here) for evidence. As *Ybarra* stated: "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*." *Ybarra*, 444 U.S. at 91 (emphasis added). The geofence warrant authorized obtaining evidence from

Google about a crime scene; it did not authorize the arrest, search, or seizure of any person.

Ybarra is thus an exception to the general rule for search warrants, which is that "a lawful search of fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search." *United States v. Ross*, 456 U.S. 798, 820-21 (1982). *Pringle*, *Ybarra*, and their progeny do not apply here because no persons were arrested, searched, or seized pursuant to the geofence warrant. Here, the warrant affidavit established a fair probability that Google had evidence of the bank robbery in its records which it accessed and used to provide services to its users and advertisers, and that probable cause supported issuance of the geofence warrant.

Illinois v. Lidster, 540 U.S. 419 (2004), further demonstrates that the Fourth Amendment permits investigators to collect identity information of those present at crime scenes. In *Lidster*, the Court held that police did not violate the Fourth Amendment when they set up a roadblock to briefly seize all motorists at the scene of a hit-and-run a week after the crime, for the primary purpose of finding witnesses. *See id.* at 423, 428. The Court found that the roadblock was "appropriately tailored ... to fit important criminal investigatory needs" and that the stops "interfered only minimally with liberty of the sort the Fourth Amendment

seeks to protect." *Id.* at 427. It would be very strange for the Fourth Amendment to allow physical stops, without individualized suspicion, of all persons at a crime scene a week after the crime, but not allow issuance of a search warrant to obtain direct crime-scene evidence, without the physical seizure of any person, merely because the crime scene information revealed the presence of persons other than the perpetrators.

Although no other federal appellate court has yet considered Google geofence warrants, the Eighth Circuit in *United States v. James*, 3 F.4th 1102 (8th Cir. 2021), held that a series of cell tower dump warrants used to solve a series of robberies complied with the Fourth Amendment. Cell tower dump warrants are similar to geofence warrants, insofar as they require a phone company to provide the government with information about all cellular devices that used cell towers in the vicinity of a crime, but their geographic coverage is typically much larger than geofence warrants.[8] Probable cause was stronger in this case than in *James*, because investigators there lacked direct evidence that the robber carried a cell phone. *See id.* at 1105. Nevertheless, the Eighth Circuit concluded that probable cause supported the tower dump warrants in *James* because the affidavits

[8] For example, the cell-sites in *Carpenter* placed the defendant in sectors "ranging from one-eighth to four square miles." *Carpenter*, 138 S. Ct. at 2218. The geofence here covered less than 0.03 square miles.

established that there was a series of crimes committed by the same individual, and that "there was 'a fair probability' that the cellular-tower records would identify the robber." *Id*. *James*'s probable cause analysis supports the issuance of the geofence warrant in this case.

Finally, Defendant challenges the inferences that supported the geofence warrant; he argues that there was "no evidence that "the robber's data was 'in fact' in Google's Sensorvault." Appellant Chatrie's Opening Brief at 29 (hereinafter "AOB"). But all that is required for probable cause is a fair probability that evidence will be found in the place to be searched. *See Gates*, 462 U.S. at 238. In addition, a magistrate may "draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant." *Id.* at 240. 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 Defendant cites no contrary case law. For example, in *United States v. Jones*, 942 F.3d 634, 639-40 (4th Cir. 2019), this Court 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.

B. The geofence warrant was sufficiently particular.

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)). And the particularity requirement may be satisfied by specifying that officers may seize evidence related to a particular crime, such as bank robbery. *United States v. Cobb*, 970 F.3d 319, 328 (4th Cir. 2020). Here, the geofence warrant satisfied these requirements.

The geofence warrant specified with precision the items to be seized: two hours of location information associated with electronic devices that were, during the 30 minutes on either side of a bank robbery, within 150 meters of a specified point. JA116-JA117. In addition, the warrant was sufficiently particular because it was appropriately constrained based on location, dates, and times. The geofence boundary was based on specific features of the site of the robbery. It covered the bank and nearby parking areas, and it went up to but did not reach major roads.

JA117, JA940. A smaller geofence could have missed where the robber and any potential accomplices parked. In addition, the duration of the geofence enabled investigators to distinguish between the robber, potential co-conspirators, victims, and other witnesses. For example, investigators could determine whether the robber met elsewhere with others from the crime scene, either shortly before or after the robbery. Thus, the warrant was appropriately tailored toward its investigatory purpose, which was to obtain evidence to help identify and convict the robber and any accomplices.

The Eight Circuit's decision in *James* further confirms that the warrant here was not overly broad. Although tower dump warrants typically cover broader areas than geofence warrants, the court held that the tower dump warrants were appropriately "constrained—both geographically and temporally—to the robberies under investigation." *James*, 3 F.4th at 1106. In particular, because the tower dumps "covered only the cellular towers near each robbery" for a "narrow and precise" 90-minute period, "the warrants were 'sufficiently definite' to eliminate any confusion about what the investigators could search." *Id.* This reasoning applies here. Indeed, the location information obtained from Google was narrower than the location information in *James*. The 150-meter radius of the geofence warrant is smaller than most individual cellular sites, and the government obtained

location information regarding only19 individuals, rather than hundreds or thousands.

The district court faulted the warrant because of the discretion the court found in the second and third steps of its three-step process, JA1376-JA1377, but the warrant appropriately directed officers to narrow down the list of accounts by comparing information from each account "against the known time and location information that is specific to this crime." JA116-JA117. This requirement functioned as an additional limitation in what was already a sufficiently limited warrant. The warrant affidavit at the outset established probable cause for all the information 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.

Although the investigators here could have and did narrow the information obtained from Google, the Fourth Amendment did not require that step because the geofence warrant was supported by probable cause to seize two hours of location and identity information for anyone at the site of the robbery during a one-hour interval. Rather than violating the Fourth Amendment, the three-step process

imposed an additional mechanism to further limit collection of information consistent with the needs of the investigation. As one magistrate judge explained in issuing a geofence warrant, "the 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." *In re Search Warrant Application*, 497 F. Supp. 3d 345, 362 (N.D. Ill. 2020).

Finally, even if there were a particularity problem with the second step in the three-step process for the geofence warrant, the appropriate remedy would at most be to sever the paragraphs of the warrant mandating the second step and to suppress second-step information.[9] "Under the severance doctrine, the constitutionally infirm portion of a warrant—usually for lack of particularity or probable cause—is separated from the remainder and evidence seized pursuant to that portion is suppressed; evidence seized under the valid portion may be admitted." *Cobb*, 970 F.3d at 330 (internal quotation marks omitted).

Here, the first step of the geofence warrant targeted narrow and clearly

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

defined information, and it had no discretionary component. In addition, first-step information alone was sufficient for investigators to recognize that Defendant's account likely belonged to the robber. JA966-JA967. Thus, even if this Court were to sever the warrant and suppress second-step information from Google, the subsequent investigation of Defendant would not be the fruit of the poisonous tree.

Defendant complains that the warrant required Google to filter its entire Location History database to find location information responsive to the warrant, which he analogizes to a search of a multi-unit building, AOB at 27-29, but this objection is without merit. In the context of geofence warrants, "the relevant question is not how Google runs searches on its data, but what the warrant authorizes the Government to search and seize." *United States v. Rhine*, 2023 WL 372044, at *28 (D.D.C. Jan 24, 2023) (upholding geofence warrant). Otherwise, "no doubt many search warrants and most third-party subpoenas for protected records would be unconstitutionally overbroad because they necessarily would require the third party to search some group of records larger than those specifically requested, whether they reside in a file cabinet or on a server." *Id.* Filtering a large database to find a narrow set of information 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. McCann*, 403 F.3d 908, 910 (7th Cir. 2005).

The nature and uses of Google's Location History database confirm that it is appropriate for a warrant to seek a narrow subset of information from within that database. Google accesses this information freely to provide users and advertisers with location-based services. Geofence warrants are similar to radius targeting advertising and measurement of store visit conversions, as they involve determinations of whether users' devices are in specific locations at specific times. The Fourth Amendment does not prohibit Google, in response to a warrant, from filtering information in a manner similar to the way it uses the same information for its own business purposes.

Moreover, Google's filtering 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. JA819-JA820. Such a database would enable Google to comply with a geofence warrant—and produce the same data that 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, which are 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.

Here, the appropriate measure for the breadth of the geofence warrant is the records sought by the warrant, not the size or organization of Google's Location History database.

Defendant asserts that the warrant left too much discretion to Google, AOB at 36, but again he is mistaken. The warrant left no discretion to Google, and Defendant points to no language in the warrant to the contrary. It is true that when a third-party provider is required to disclose records pursuant to any warrant, it may refuse and 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 itself was insufficiently particular.

Defendant argues that the warrant was insufficiently particular because investigators "did not have any suspects" and "valid warrants do not work that way." AOB 37. Again, *Zurcher* demonstrates that he is wrong. A warrant may be used to investigate crime before officers identify a suspect, provided that "it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises." *Zurcher*, 436 U.S. at 559. Most warrants may involve seizure of evidence from the person suspected of crime, but under *Zurcher*, the Fourth Amendment does not forbid using a warrant to solve a crime, and Defendant points to no case to the contrary. *See United States v. Long*, 774 F.3d 653, 659 (10th Cir. 2014) ("And we know of no authority that officers

cannot search a place where there is likely to be contraband or evidence of a crime unless they can identify the likely perpetrator.").

Defendant references "First Amendment concerns" with the warrant, AOB at 35, but *Zurcher* held that the Fourth Amendment standards of probable cause and particularity govern even warrants that raise significant First Amendment concerns. *See Zurcher*, 436 U.S. at 565 ("courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search"). Here, 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 First and Fourth Amendments under the standards of *Zurcher* because it was issued based on probable cause and specified its objects with particularity.

III. The good-faith doctrine precludes suppression.

Even if Defendant could identify a Fourth Amendment flaw in the search warrant, and even if Defendant could establish a protected Fourth Amendment interest in the information disclosed by Google, 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.

A. TFO Hylton reasonably relied on the geofence warrant.

Suppression is inappropriate under the good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984). When officers 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 "an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; (2) 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"; (3) when "the issuing magistrate wholly abandoned his judicial role"; and (4) 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." *Leon*, 468 U.S. at 923; *United States v. Perez*, 393 F.3d 457, 461 (4th Cir. 2004). These circumstances are not present in this case.

1. The warrant was not so lacking in probable cause as to render reliance on it unreasonable.

Defendant argues that the warrant was based on a "bare bones" affidavit and "completely devoid" of probable cause, AOB at 23, but the affidavit demonstrates otherwise. 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). As explained above, the warrant was supported by probable cause because the affidavit established that the bank robber had used a cell phone, and it explained why there was a fair probability that Google would store cell phone users' location information. *See supra* at 29-33. In addition, given the layout of the roads and parking areas surrounding the bank, the 150-meter radius of the geofence was reasonably tailored to collect evidence of the robbery. *See supra* at 37-44. That is sufficient to show that TFO Hylton's reliance on the warrant was reasonable.

As previously explained, Defendant's numerous additional objections to the probable cause that supported the warrant lack merit, and for the same reasons, TFO Hylton reasonably relied on the warrant. *See supra* at 32-36. First,

Defendant cites *Pringle*, *Ybarra*, and related cases, AOB at 26, but the probable cause standards of *Pringle* and *Ybarra* do not apply to a geofence warrant because a geofence warrant does not involve an arrest, search, or seizure of a person. *See supra* at 32-34. But even if this Court ultimately decides that *Pringle* and *Ybarra* govern geofence warrants, TFO Hylton could reasonably have relied on the warrant, given the probable cause standard of *Zurcher* and the lack of case law applying *Pringle* and *Ybarra* to geofence warrants.

Second, although Defendant analogizes Google to a multi-unit building, AOB at 27, the warrant appropriately required Google to disclose particular information. *See supra* at 41-43. Moreover, given the lack of contrary precedent, it was not unreasonable for TFO Hylton to rely on the warrant based on the actual information sought by the warrant, rather than on Google's internal filtering processes.[10]

Third, Defendant challenges the inferences that supported the geofence warrant, AOB at 29, but his challenge is meritless because a magistrate may "draw

[10] Defendant also complains that although "the warrant ostensibly sought data about people around the time of the bank robbery," it listed Google as the place to be searched, "almost a month after the robbery." AOB at 28. On this point, the warrant is correct about the place to be searched and things to be seized: like the warrant in *Zurcher*, which authorized a search of a newspaper for evidence of a crime that occurred elsewhere, the warrant here was properly directed to Google, as it too held evidence of a crime that occurred elsewhere.

such reasonable inferences as he will from the material supplied to him by applicants for a warrant." *Gates*, 462 U.S. at 240; *see supra* at 36. Here, where the probable cause that supported the warrant was based on a combination of specific facts (including that the robber carried a cell phone) and reasonable inferences regarding why Google would store evidence of the phone's location, TFO Hylton's reliance on the warrant was reasonable.

2. The warrant was not facially deficient.

Nor was the warrant so facially deficient that officers could not reasonably rely on it. *See supra* at 37-44. Defendant asserts that it "failed to limit the data searched and seized," AOB at 34, but in fact it was specifically tailored in both time and space. The warrant was limited to disclosure of location information over a two-hour interval, as well as accompanying identity information, for devices present in a 150-meter radius at the site of the robbery during a one-hour interval. Those limitations are more than sufficient for an officer to reasonably rely on the facial validity of the warrant.

Nor did the warrant's further requirement that officers attempt to narrow down the information obtained from Google render TFO Hylton's reliance on the warrant unreasonable. *See supra* at 39-40. This requirement functioned as an additional limitation on an already limited warrant. There was probable cause to obtain identity information and two hours of location data for all individuals

present at the site of the robbery during the hour of the robbery, and so investigators' further limiting the information collected within those narrow parameters is consistent with the Fourth Amendment. At a minimum, the warrant was therefore not so facially deficient that officers could not reasonably rely on it.

3. The magistrate did not abandon his judicial role.

Defendant asserts that the magistrate abandoned his judicial role, but his argument simply repeats his meritless assertions that the warrant was lacking in probable cause and particularity. AOB at 38-39. Defendant cites *Lo-Ji Sales v. New York*, 442 U.S. 319 (1979), but unlike here, that case provides an example of what it means for a magistrate to abandon his judicial role: the magistrate there accompanied officers executing the warrant and determined what could be seized, thereby becoming "a member, if not the leader, of the search party which was essentially a police operation." *Id.* at 327. Here, the magistrate stayed within his judicial role—he reviewed the affidavit and issued the search warrant. Furthermore, for the reasons discussed previously, the warrant was not facially deficient or so lacking in probable cause that investigators' reliance on it was unreasonable. *See supra* at 29-44.

4. Defendant waived any *Franks* challenge to the warrant.

Defendant argues for suppression based on alleged omissions from the affidavit, AOB at 32-33, but Defendant waived this argument below, and he may

not raise it on appeal. "A party who identifies an issue, and then explicitly withdraws it, has waived the issue." *United States v. Robinson*, 744 F.3d 293, 298 (4th Cir. 2014) (quoting *United States v. Rodriguez*, 311 F.3d 435, 437 (1st Cir. 2002)). "And when a claim is waived—as opposed to forfeited—it is not reviewable on appeal, even for plain error." *Morehouse*, 34 F.4th at 395 (internal quotation marks omitted).

Under *Franks v. Delaware*, 438 U.S. 15 (1978), omissions from a warrant provide a basis for suppression when a defendant proves "the affiant intentionally or recklessly omitted material information from the affidavit." *United States v. Pulley*, 987 F.3d 370, 376 (4th Cir. 2021). Below, in his final brief supporting his suppression motion, Defendant explicitly disclaimed reliance on *Franks*: "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." JA1115. On appeal, he fails to acknowledge his waiver, and instead argues that "[t]his Court could also find that Det. Hylton recklessly omitted material information in violation of *Leon* and *Franks v. Delaware*." AOB at 11 n.2 and 32 n.5. Because Defendant waived reliance on *Franks*, this Court must reject his attempt to raise it now.

Moreover, even if Defendant had not waived his *Franks* argument, it is without merit. The Defendant faults TFO Hylton for not informing the magistrate about Google's internal data filtering processes, AOB at 32-33, but TFO Hylton lacked prior knowledge about those facts, JA1023, and Google's internal data processing lacks Fourth Amendment significance. *See supra* at 41-43. Defendant also faults TFO Hylton for not disclosing "the true scope of the number of people to be searched and true boundaries of the 'geofence,'" AOB at 33, but the warrant did disclose its boundaries, and there was no way for TFO Hylton to know ahead of time exactly how many users would fall within it. And to the extent that Defendant is arguing that the affidavit should have addressed potential inaccuracies in Google's location information, the fact that there is imprecision in cell phone location measurements is common knowledge, and TFO Hylton could reasonably have expected the issuing magistrate to be aware of that fact. Nor would potential inaccuracies in location data affect the existence of probable cause—potential inaccuracies would ultimately go to the weight of location

information at trial, not its admissibility.[11] In sum, the record does not support Defendant's allegation that TFO Hylton "appeared to have no real understanding of geofence warrants." AOB at 31. TFO Hylton chose appropriate temporal and physical bounds for the geofence, supported the warrant with probable cause, and obtained evidence from Google within the scope of the warrant.

5. The geofence warrant was not a general warrant.

The geofence warrant was not a general warrant, as it was supported by probable cause and specified its object with particularity. *See supra* at 29-44. In addition, Defendant errs by attempting to invent a new rule to avoid *Leon*'s good-faith analysis: Defendant asserts that good-faith doctrine should not apply where a court deems a warrant to be a "general warrant." AOB at 46-49. But the good-faith exception depends on whether the officer reasonably relied on a warrant, not on how the reviewing court labels it. Defendant cites case like *United States v. George*, 975 F.2d 72, 77-78 (2d Cir. 1992), in which the court suppressed evidence

[11] Defendant also exaggerates the actual extent of the uncertainty in Google's location measurements. He emphasizes that in Step 1, a single measurement point for one device had an error radius of 387 meters. AOB at 7. But that same device had another measurement 23 seconds earlier at the same latitude and longitude coordinates and an error radius of only 87 meters, entirely inside the geofence. JA2104. As FBI 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 moving. JA948-JA949. The uncertainty associated with the second point does not affect the accuracy of the first.

from a warrant it called a general warrant. But *George* explicitly suppressed evidence based on *Leon*'s framework: it found the warrant "so facially deficient" that officers could not reasonably rely on it. *Id.* at 77. Where the fruits of a warrant are not suppressible under *Leon*, it would be inconsistent with *Leon* to suppress evidence on the basis that the court describes the warrant as a "general warrant."

B. TFO Hylton reasonably relied on a warrant and consulted with counsel before using a new investigative technique.

When TFO Hylton sought the warrant in this case, geofence warrants were a new investigative technique, and there were no judicial opinions analyzing them under the Fourth Amendment. In *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), this Court rejected suppression in analogous circumstances. *McLamb* 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, TFO Hylton did what this Court expects under *McLamb*. He consulted with prosecutors about geofence warrants before seeking both state and federal geofence warrants. JA1021-JA1022. He had previously obtained geofence warrants from both state judges and a United States Magistrate Judge. JA1020-JA1021. No prosecutor or judge had ever found a problem with these warrants. JA1021-JA1022. In this investigation, he then sought and obtained a search warrant from a state magistrate. In sum, he behaved reasonably for an investigator seeking to employ a new investigative technique.

Defendant objects that TFO Hylton had received no training on geofence warrants, AOB at 30, but there is no indication in *McLamb* that the agents had received training on darknet child pornography warrants. Indeed, such trainings may not exist when a new investigative technique first arises. *McLamb* calls for consultation with prosecutors and then seeking a warrant, not meeting a bureaucratic training requirement. Consulting directly is an effective form of training, even if it is not officially categorized as such. As the district court recognized, TFO Hylton did what *McLamb* calls for, and the good-faith exception

therefore applies.[12]

Recent judicial opinions provide further evidence that TFO Hylton's reliance on the warrant was reasonable: numerous judges have issued or upheld geofence warrants, and if they have all been mistaken, it was reasonable for TFO Hylton to be mistaken as well. *See United States v. Workman*, 863 F.3d 1313, 1321 (10th Cir. 2017) (stating that if eight federal judges were mistaken in upholding a particular warrant, investigators "could reasonably have made the same mistake"). United States Magistrate Judges have issued opinions explaining why they issued geofence warrants. *See, e.g.*, *In re Search Warrant Application*, 497 F. Supp. 3d 345 (N.D. Ill. 2020); *In re Search of Information*, 579 F. Supp. 3d 62 (D.D.C. Dec. 30, 2021). District courts have denied geofence suppression motions and held that the geofence warrants complied with the Fourth Amendment. *See Rhine*, 2023 WL 372044, at *32; *United States v. Anthony*, No. 1:21-CR-128, ECF No. 125 at 31 (W.D. Mich. Mar. 1, 2022) (orally denying motion to suppress ten geofence warrants and stating "the warrants challenged here with respect to the geofences at

[12] Defendant objects that TFO Hylton consulted with prosecutors for the prior geofence warrants, but the record demonstrates that he discussed a new investigative technique—geofence warrants—with prosecutors, and he was never told that they were illegal. JA1021-JA1022. Defendant further objects that TFO Hylton had not yet received data from Google in response to his prior geofence warrants, AOB at 41, but that does not affect the fact that Hylton knew that other judges, including a United States Magistrate Judge, had considered and approved his similar geofence warrant applications. JA1020-JA1021.

issue do satisfy traditional probable cause and particularity standards," except for one state warrant that was "a little sparse on some of the information regarding social media," but still sufficient for *Leon* good faith). And the Eighth Circuit approved cell tower dump warrants based on reasoning that supports geofence warrants. *James*, 3 F.4th at 1105-06. If all of these courts have erred, TFO Hylton could reasonably have made the same mistake and reasonably relied on the magistrate's decision to issue the warrant.

Conclusion

For the foregoing reasons, this Court should affirm the denial of Defendant's motion to suppress.

Respectfully submitted,

Jessica D. Aber
United States Attorney

By: /s/

Nathan Judish
Senior Counsel, Computer Crime and Intellectual Property Section
United States Department of Justice
1301 New York Ave., NW
Washington, DC 20530
(202) 616-7203
Nathan.judish@usdoj.gov

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
Kenneth.Simon2@usdoj.gov

Statement Regarding Oral Argument

The United States does not oppose Defendant's request for oral argument.

Certificate of Compliance

I certify that this brief was written using 14-point Times New Roman typeface and Microsoft Word 2016.

I further certify that this brief does not exceed 13,000 words (and is specifically 12845 words) as counted by Microsoft Word, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

I understand that a material misrepresentation can result in the Court's striking the brief and imposing sanctions.

/s/

Nathan Judish
Senior Counsel, Computer Crime
and Intellectual Property Section