

No. 22-4489

**IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT**

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)**

PETITION FOR REHEARING EN BANC

MICHAEL W. PRICE
**National Association of Criminal
Defense Lawyers**
**Litigation Director, Fourth
Amendment Center**
1660 L Street NW, 12th Floor
Washington, DC 20036
(202) 465-7615
mprice@nacdl.org

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800
laura_koenig@fd.org

Counsel for Appellant

TABLE OF CONTENTS

Table of Authorities	ii
Introduction	1
Background	2
Reasons for Granting the Petition	6
I. The Privacy of Location History Data and the Constitutionality of Geofence Warrants Are Questions of Exceptional Importance	6
A. Geofence Warrants Present Novel Issues of Far-Reaching Importance	6
B. The Panel Majority Opinion Sows Confusion	9
II. The Panel Majority Opinion Conflicts With <i>Carpenter</i> , <i>Leaders</i> , and <i>Smith</i>	10
A. The Panel Majority Opinion Mechanically Applies the Third-Party Doctrine and Conflicts With <i>Carpenter</i>	10
B. The Panel Majority Opinion Conflicts With <i>Leaders of a Beautiful Struggle</i>	15
C. The Panel Majority Opinion Conflicts with the Fifth Circuit	17
Conclusion	18
Request for Rebriefing	18
Certificate of Compliance	19

TABLE OF AUTHORITIES

Cases

<i>Carpenter v. United States</i> , 585 U.S. 296 (2018)	passim
<i>In re Search of Information that is Stored at the Premises Controlled by Google</i> , 579 F.Supp.3d 62 (D.D.C. 2021)	9
<i>Leaders of a Beautiful Struggle v. Baltimore Police Dep’t</i> , 2 F.4th 330 (4th Cir. 2021).....	2, 10, 15, 16, 17
<i>People v. Seymour</i> , 536 P.3d 1260 (Colo. 2023)	8
<i>United States v. Easterday</i> , No. CR-22-404, 2024 WL 195828 (D.D.C. Jan. 18, 2024).....	9
<i>United States v. Jones</i> , 565 U.S. 400 (2012).....	7, 17
<i>United States v. Kirkendoll</i> , No. 1:22-CR-00361, 2024 WL 1016049 (D.N.M. Mar. 8, 2024)	9
<i>United States v. Knotts</i> , 460 U.S. 276 (1983)	12, 14
<i>United States v. Miller</i> , 425 U.S. 435 (1976).....	10, 11
<i>United States v. Rhine</i> , 652 F.Supp.3d 38 (D.D.C. 2023).....	9
<i>United States v. Smith</i> , No. 23-60321, 2024 WL 3738050 (5th Cir. Aug. 9, 2024).....	passim
<i>United States v. Wright</i> , No. CR-419-149, 2023 WL 6566521 (S.D. Ga. May 25, 2023).....	9

Rules

Fed. R. App. P. 35(b)(1).....	1
-------------------------------	---

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

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)

PETITION FOR REHEARING EN BANC

INTRODUCTION

Okello Chatrie petitions for rehearing en banc. The full court should review the panel’s decision because it involves questions of exceptional importance and conflicts with decisions of the Supreme Court, this Court, and another Court of Appeals. *See* Fed. R. App. P. 35(b)(1)(A), (B).

A geofence search is a novel surveillance tool that searches location data within the accounts of millions of Google users, including Chatrie. The panel opinion fails to appreciate the intensely revealing nature of geofence searches—likening them to

beepers—and ignores the test in *Carpenter v. United States*, 585 U.S. 296 (2018). It “mechanically” applies the 1970s-era “third-party doctrine” to a sophisticated new surveillance technology, *id.* at 298, narrows *Carpenter* to irrelevance, and conflicts with the Fifth Circuit, *see United States v. Smith*, No. 23-60321, 2024 WL 3738050, at *1 (5th Cir. Aug. 9, 2024) (hereinafter “*Smith*”), as well as this Court’s decision in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (en banc).

BACKGROUND

In May 2019, someone robbed the Call Federal Credit Union in Midlothian. J.A. 1328. Without suspects, police “turned to geofence technology.” J.A. 1349. The “geofence” sought “location data for every [Google location history] user within a particular area over a particular span of time.” J.A. 1327-1328. Here, that meant a 17.5-acre circle encompassing the bank, a church, restaurant, hotel, apartment complex, self-storage facility, senior living home, two busy streets, and several residences. J.A. 1351-1357.

Pursuant to the warrant, police made Google scour user accounts for “Location History.” J.A. 1331. Google considers Location History “a journal stored primarily for the user’s benefit” and “not a business record.” J.A. 1330. Location History “can estimate a device’s location down to three meters” and tell “where a device is in terms of elevation.” J.A. 1332, J.A. 1334. It “logs a device’s location, on average, every

two minutes,” J.A. 1332, even if the phone is unused and even if the user deletes the app that originally enabled Location History, J.A. 1334. “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.” J.A. 1334. By 2018, “[n]umerous tens of millions” of Google users had enabled Location History. J.A. 1331.

Chatrie enabled Location History in July 2018, likely through “Google Assistant.” J.A. 1340. In 2018, Google’s interface said Location History “[s]aves where you go with your devices,” providing optional further detail in a “[d]eceptive click-flow.” J.A. 1339, J.A. 1343. One Google employee said it appeared “‘designed to make things possible, yet difficult enough that people won’t figure ... out’ how to turn Location History off.” J.A. 1342.

In 2018, Google worked with “law enforcement agencies, including the Computer Crime and Intellectual Property Section of the United States Department of Justice ... to develop internal procedures on how to respond to geofence warrants.” J.A. 1344. First, “Google must ‘search ... all [Location History] data to identify users’ whose devices were present within the geofence during the defined timeframe.” J.A. 1345. Second, without court review, “law enforcement ... ‘can compel Google to provide additional ... location coordinates *beyond* the time and geographic scope of the original request.’” J.A. 1347. Third, also without court review, “the [G]overnment

can compel Google ... to provide *account-identifying information* for the users ‘the [G]overnment determines are relevant to the investigation.’” J.A. 1348.

Police initially obtained Location History for nineteen users across “210 individual location points.” J.A. 1354. They then obtained additional Location History for a longer period for nine users, and finally account subscriber information for three users. J.A. 1355-1356. “Ultimately, the [geofence] information law enforcement obtained led the authorities to Chatrie.” J.A. 1359. A grand jury indicted Chatrie for armed robbery and brandishing a gun during the robbery. J.A. 1359-1360. Chatrie filed a suppression motion. J.A. 25.

Finding that the warrant “plainly violates” the Fourth Amendment, the district court denied Chatrie’s suppression motion, concluding that the good-faith exception applied. J.A. 1328, J.A. 1388-1389. The district court assumed “that the Government’s collection of data here is a ‘search’” because it obtained a warrant and argued its validity. J.A. 1368. It also found that “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.” J.A. 1365. Finally, while declining to conclusively decide the question, the court was “unconvinced that the third-party doctrine would render hollow Chatrie’s expectation of privacy in his data, even for ‘just’ two hours.” J.A. 1379.

The panel majority affirmed the district court’s denial of Chatrie’s suppression motion on different grounds. Specifically, the panel found “that the government did not conduct a Fourth Amendment search when it obtained two hours’ worth of Chatrie’s location information, since he voluntarily exposed this information to Google.” Op. 3. The majority thus rejected the district court’s factfinding on the lack of “meaningful” consent in the opt-in process for Location History. *See* J.A. 1380.¹

Judge Wynn dissented, concluding that “the intrusion was a search that triggered the Fourth Amendment’s protections.” Dissent 36. Judge Wynn reasoned that “[a] faithful reading of *Carpenter*—not to mention common sense—compels the conclusion that when the police obtained Chatrie’s Location History data, they engaged in a Fourth Amendment search.” *Id.* at 53. The Supreme Court has acknowledged “the third-party doctrine is an increasingly tenuous barometer for measuring an individual’s privacy expectations in the digital era.” *Id.* at 45. “The sharing of Location History is likewise not ‘meaningfully’ voluntary ... because it is conveyed automatically every two minutes” and once enabled, “it is automatically conveyed *across all devices* on which a user is logged into Google, even when the

¹ Following oral argument, Google announced that it would no longer store users’ Location History, which instead would be stored on users’ devices. *See* ECF 62. This change may prevent police from obtaining geofence warrants from Google in the future, but it does not moot Chatrie’s case or any other pending geofence challenge.

user has deleted the Google app through which they opted into Location History.” *Id.* at 70-71.

REASONS FOR GRANTING THE PETITION

I. The Privacy of Location History Data and the Constitutionality of Geofence Warrants Are Questions of Exceptional Importance

The panel majority opinion allows police to use an Orwellian surveillance tool without a warrant, at least for two hours at a time. If obtaining location history is not a search, surveillance by the Executive Branch of anyone with Location History enabled on a cell phone for at least two hours—such as political dissidents, women seeking reproductive healthcare, reporters, politicians, and judges—is fully within its power without judicial check. The decision has dystopian implications for the privacy of location information and other personal data stored with technology companies.

A. Geofence Warrants Present Novel Issues of Far-Reaching Importance

Geofence warrants require searches of “numerous tens of millions” of users in the hopes of identifying a criminal suspect. J.A. 1331. They are novel because, unlike normal warrants, geofence warrants operate in reverse: search first, individualized suspicion later. They rely on Location History data, a potent source of personal location information imaginable only in the digital age, allowing police to “time travel” as if they had been tailing millions of Americans for years. Dissent 61. Indeed, the premise is that anyone with a phone could be a suspect, so warrants simply describe the alleged

crime location and make Google identify user accounts within some proximity during a relevant time.

Never have police been able to see into the past with such clarity or ease. Geofences are massive digital dragnets, incomparable to any physical search and one of the most powerful digital surveillance tools in existence. But the panel majority gives police this power without check, for hours or days at a time. Dissent 103; *id.* at 99 (“[T]he majority opinion enacts a sweeping new rule: when it comes to data like Location History, police are only required to obtain warrants for longer intrusions—without any regard for the advancing capabilities of the surveillance technologies that police may use or the revealing nature of the data that the police may access.”).

In fact, the use of geofences has not been confined to “egregious or violent” crimes. *Smith* at *2. Rather, police have frequently used them to investigate even minor, nonviolent offenses. *Id.* (“Law enforcement officials have obtained geofence warrants for investigations into stolen pickup trucks and smashed car windows.”). Indeed, the use of geofence warrants has “skyrocketed” since 2016, Op. 6, such that a quarter of all warrants issued to Google in 2022 were geofences. J.A. 1344. Rejecting the warrant requirement here is “akin to inviting governmental abuse.” Dissent 101 (citing *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring)).

Finally, the majority opinion calls into doubt the privacy afforded to other types of personal data that people store with companies like Google. The majority did not

merely hold that the geofence warrant was proper, or that the good-faith exception applied. Instead, it held that Chatrue had *no Fourth Amendment protection* in his Location History data because he kept it with Google. But there is nothing special about Location History data compared to other information that people store with Google.

The same third-party logic would apply to emails, photos, and documents in a Google account. Or to Google search history. *See, e.g., People v. Seymour*, 536 P.3d 1260, 1273 (Colo. 2023) (holding that there is a “reasonable expectation of privacy in ... search [engine] history”). It includes data generated by “Fitbit and Apple watches, health apps, journal apps (such as iPhone’s built-in Notes App), apps for tracking menstrual cycles, ChatGPT, and smart cars, and [] technologies [that] record the most intimate, retrospective information[.]” Dissent 72. There is no limiting principle, and no reason the panel’s rationale does not apply equally to email, pictures, or search history—provided it’s just a quick peek.

The majority opinion now permits police to “surreptitiously surveil places of worship, protests, gun ranges, abortion or drug-rehabilitation clinics, union meetings, marital counseling or AA sessions, and celebrations of cultural heritage or LGBTQ+ pride, among numerous other types of sensitive places or gatherings—with no judicial oversight or accountability.” Dissent 102. The full court should grant rehearing to address these novel and weighty Fourth Amendment concerns affecting millions of people across the country.

B. The Panel Majority Opinion Sows Confusion

Before the panel majority’s opinion, the operating assumption for police, Google, and federal courts was that a warrant is required for a geofence search of any duration. Indeed, police obtained a warrant in this case, J.A. 1349, as they have done thousands of other times, J.A. 1343-44, according to a process that the Department of Justice crafted with Google. J.A. 1344; Op. 7. Google has consistently required a warrant to search a user’s Location History, just as it does for other types of account “contents,” because Location History effectively is “the contents of a user’s written journals stored on Google Drive.” J.A. 139. Likewise, federal courts have assumed a warrant is required, focusing instead on the constitutionality of the search at issue. *See, e.g., United States v. Rhine*, 652 F.Supp.3d 38, 81 (D.D.C. 2023) (collecting cases); *United States v. Easterday*, No. CR-22-404, 2024 WL 195828, at *3 (D.D.C. Jan. 18, 2024); *United States v. Kirkendoll*, No. 1:22-CR-00361, 2024 WL 1016049, at *2 (D.N.M. Mar. 8, 2024); *In re Search of Information that is Stored at the Premises Controlled by Google*, 579 F.Supp.3d 62, 74 (D.D.C. 2021); *United States v. Wright*, No. CR-419-149, 2023 WL 6566521, at *18 n.23 (S.D. Ga. May 25, 2023).

The panel opinion upends the consensus that the warrant requirement applies based on the premise that the government “did not conduct a Fourth Amendment search” when it searched two hours of Location History data. Op. 35. But the opinion provides little guidance on what duration of geofence surveillance, if any, *would*

constitute a search. Dissent 103 (“For the first time since the ratification of the Fourth Amendment, the government is permitted to retroactively surveil American citizens anywhere they go—no warrant needed—so long as it keeps its snooping to a few hours or perhaps a few days.”).

In sum, the majority opinion creates confusion as to when judicial oversight is warranted, while eliminating any judicial check on police surveillance for “short-term” intrusions. Op. 17, 26-27, 29 n.23. Rehearing is necessary to clarify that a warrant is required to search Location History and address the overbreadth and particularity problems inherent in geofences.

II. The Panel Majority Opinion Conflicts with *Carpenter*, *Leaders*, and *Smith*

The panel opinion conflicts with the Supreme Court’s decision in *Carpenter* as well as this Court’s decision in *Leaders*. It also splits with the Fifth Circuit’s decision in *Smith*, which not only held that the Fourth Amendment protects user Location History, but also that geofence warrants are “modern-day general warrants,” “categorically prohibited by the Fourth Amendment.” *Smith* at *16, 18.

A. The Panel Majority Opinion Mechanically Applies the Third-Party Doctrine and Conflicts with *Carpenter*

As an initial matter, the third-party doctrine provides that the Fourth Amendment generally does not protect *business records* voluntarily turned over to third parties. *United States v. Miller*, 425 U.S. 435, 442-43 (1976). Google’s location history data, however, is private, user-controlled, and password-protected, just like any picture or

email stored in the cloud, and unlike the CSLI records “generated for commercial purposes” at issue in *Carpenter*. 585 U.S. at 311.

Even in the context of business records, however, *Carpenter* warned against “mechanically applying” the third-party doctrine to novel surveillance technologies. *Id.* at 298. Noting that the third-party doctrine does not account for “seismic shifts in digital technology,” *Carpenter* observed “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.* at 313-14.

Nonetheless, the panel found that the third-party doctrine “squarely governs” here, Op. 22, misreading *Carpenter* as if it had imposed a seven-day “cutoff” on Fourth Amendment rights. *Carpenter*, 585 U.S. at 310 n.3. The Supreme Court said no such thing.

Carpenter didn’t give a free pass to short-term government surveillance of CSLI, because it explicitly reserved that question. *See id.* Instead, in evaluating the *business records* at issue, *Carpenter* required consideration of not only search duration, but also the nature of the data being searched. *Id.* at 314; Dissent 65-66 (“[*Carpenter*] clearly focused on the character of the search, rather than its length”). But the panel did not do so here. Instead of considering the factors *Carpenter* articulated, the panel likened Location History to CSLI and collapsed the analysis into a question of duration alone,

erroneously concluding that two hours of Location History data “was plainly insufficient” under *Carpenter*. Op. 29.

Even if it constituted business records, two hours of Location History data is even more revealing than the CSLI at issue in *Carpenter*. Dissent 53-54. Location History is far more “*precise*” and frequently collected than CSLI, capable of automatically locating users “within *meters*,” including the “*floor in a building* where a person might be,” every two minutes. *Id.* at 54-56. As a result, it creates the kind of “near perfect surveillance” that *Carpenter* feared. *Id.* at 54 (quoting *Carpenter*, 585 U.S. at 312).

Second, the panel wrongly concluded that the geofence search here is akin to the “short-term [surveillance of] public movements in *Knotts*.” Op. 19-20. *Knotts* involved the use of a “rudimentary” tracking device physically installed by officers and followed in real-time to surveil a pre-identified suspect. *United States v. Knotts*, 460 U.S. 276, 278 (1983); Dissent 66. By contrast, there was no preexisting suspect in this case. The geofence simply “pulled from a preexisting database of users’ past movements,” which allowed police to effectively “time travel” as if they had been tailing “numerous tens of millions” of people for years. Dissent 61. Like *Carpenter*, “each user [had] ‘effectively been tailed’ since they activated Location History.” *Id.*

Third, the panel failed to consider the “intimacy” implicated by two hours of Location History, which Google likens to a “virtual journal.” J.A. 128. Location

History “faithfully follows” users inside constitutionally protected spaces, Op. 59 (quoting *Carpenter*, 585 U.S. at 311), and could “tour a person’s home, capture their romantic rendezvous, accompany them to any number of medical appointments, political meetings, strikes, or social engagements, or otherwise begin constructing their afternoon and early-evening routines.” Dissent 63; J.A. 1359. Indeed, the geofence here encompassed a nearby church and effectively captured a hotel, an apartment complex, a senior-living facility, and several residences. Dissent 56. Thus, two hours of Location History could reveal far more about a user’s private activities than could days of the neighborhood-sized “wedge” shapes generated by CSLI. Dissent 55-56 (citing *Carpenter*, 585 U.S. at 312).

The panel erred in dismissing these qualities of Location History by noting that “the intrusion did not actually enter Chatrie’s home.” Op. 58. But such a post-hoc analysis conflicts with *Carpenter*, which instead requires considering the tool’s “capabilities during the intrusion as opposed to the specific facts of each intrusion.” Dissent 59; *see also Smith* at *12 n.8 (noting that panel’s “conclusion directly conflicts with *Carpenter*.”). As Judge Wynn recognized, “The government ... cannot circumvent the Constitution merely because, by sheer luck, its target did not stray from the safe zone.” Dissent 60.

Fourth, the majority does not account for the “ease of access” provided by geofence warrants, which “scour the continuous locations of numerous people in any

area at any time” with “just the click of a button” and “at practically no expense.” Dissent 67. Likening Location History to the beeper in *Knotts*, Op. 19-20, the majority ignores the Supreme Court’s warning that courts must take account of novel surveillance technologies and “place obstacles in the way of a too permeating police surveillance.” Dissent 46 (quoting *Carpenter*, 585 U.S. at 305); *see also Smith* at *18 (Ho, J., concurring) (“[H]amstringing the government is the whole point of our Constitution.”). Instead, the majority “mechanically appl[ies] the third-party doctrine” in defiance of the Supreme Court’s repeated and express commands not to do so.” Dissent 85 (quoting *Carpenter*, 585 U.S. at 314).

Finally, the panel majority mischaracterizes the voluntariness of the process by which Chatric opted-in to Location History. *See* Op. 20-23. In fact, his assent was likely accomplished “by selecting ‘YES, I’M IN’ at midnight while setting up Google Assistant.” J.A. 1380. Even so, whether this even matters post-*Carpenter* is unclear. *See* Dissent 68-69. Chatric’s acquiescence to Google’s prompts was no more “meaningful” than *Carpenter*’s service agreement with Sprint consenting to its CSLI use. Dissent 69. Google’s location history opt-in process was “less than pellucid,” and its warnings were “limited and partially hidden.” J.A. 1379-1380; Dissent 75. Even if Location History were used to target advertising— which it is not²—such use would

² Google “never share[s] anyone’s location history with a third party [advertiser],” and advertisers cannot obtain any identifiable information about users’ locations. J.A. 613. Nor can advertisers return to Google and ask for more information

not negate Chatrle's expectation of privacy in his Location History, just as Carpenter's contract with Sprint did not defeat his privacy interest in his CSLI. *See Carpenter*, 585 U.S. at 311.

In sum, the panel majority fails to consider the *Carpenter* factors, mechanically applies the 1970s third-party doctrine to a sophisticated new surveillance technology and mistakes a "limited disclosure to Google with an open invitation to the State." Dissent 77. The majority opinion thus conflicts with *Carpenter* and makes rehearing imperative.

B. The Panel Majority Opinion Conflicts with *Leaders of a Beautiful Struggle*

The panel opinion also conflicts with this Court's decision in *Leaders*, concerning Baltimore's use of persistent aerial surveillance to track cars on public streets. *See* 2 F.4th at 333-34. The majority maintains that *Leaders* solidified a distinction between long and short-term surveillance, noting that Baltimore kept records for a "prolonged" period of 45 days. Op. 17 (citing *Leaders*, 2 F.4th at 341). But Baltimore police were not at their desks perusing 45 days of aerial surveillance footage. Instead, they obtained only "shorter snippets" around the time of a crime, usually measured in minutes. 2 F.4th at 342.

about where certain devices were before or after seeing an ad or visiting a store. J.A. 615.

The surveillance at issue in *Leaders* was particularly troubling because police could draw on a comprehensive repository of location data, thereby generating “tracks” to observe someone’s movements retrospectively. *Id.* Like CSLI, it was a tool that “[ran] against everyone.” *Id.* at 341; *Carpenter*, 585 U.S. at 312. As a result, the length of the “track” was not decisive because police could “travel back in time” and observe someone’s movements at will. *Leaders*, 2 F.4th at 341. It “enable[d] police to ‘retrace a person’s whereabouts,’ granting access to otherwise ‘unknowable’ information.” *Id.* at 342.

A geofence warrant similarly “transcends mere augmentation of ordinary police capabilities,” akin to a time machine with no analog before the digital age. *Id.* at 345; J.A. 1362 (“this expansive, detailed, and retrospective nature of Google location data [] is unlike, for example, surveillance footage”). As the district court found, the geofence “access[ed]” an “almost unlimited pool” of “constant, near-exact location information for each user” with Location History enabled. J.A. 1362. “Numerous tens of millions” of users were searched. J.A. 1331. As in *Leaders*, without the ability to search this enormous cache of accounts, the government would not have identified Chatric. J.A. 1362; *Leaders*, 2 F.4th at 342 (“[T]he government can deduce such information only because it recorded everyone’s movements.”).

The geofence here is exactly the kind of surveillance program outlawed in *Leaders*. Because the panel opinion conflicts with *Leaders*, this Court should rehear this case en banc.

C. The Panel Majority Opinion Conflicts with the Fifth Circuit

The panel opinion also conflicts with the Fifth Circuit’s decision in *Smith*. *Smith* at *1. Because people have a reasonable expectation of privacy in short-term Location History, *Smith* held that a geofence is a search covered by the Fourth Amendment. *Id.* at *11. Moreover, *Smith* concluded that geofence warrants amount to “categorically prohibited” “general warrants.” *Id.* at *16.

First, *Smith* reasoned that Google users have an expectation of privacy in their Location History data, concluding that the privacy invasion more than matches those in *Jones* and *Carpenter*. *Smith* at *11-12. The court agreed with Judge Wynn that such “electronic opt-in processes are hardly informed and, in many instances, may not even be voluntary.” *Id.* at *13. Indeed, “users are bombarded multiple times with requests to opt in across multiple apps ... innocuously promis[ing] app optimization, rather than reveal[ing] the fact that users’ locations will be comprehensively stored in a ‘Sensorvault.’” *Id.*

Second, *Smith* observed that geofence searches “allow law enforcement to rummage through troves of location data from hundreds of millions of Google users *without any description of the particular suspect ... to be found.*” *Id.* at *15 (emphasis

added). Noting that a search without a suspect is ““emblematic of general warrants,”” the court concluded that geofence searches pose an ““alarming”” potential for ““permeating police surveillance.”” *Id.* at *11, *15. The full court should consider whether the Fourth Amendment requires this novel and enormous power of surveillance to be subject to judicial review via the warrant requirement.

CONCLUSION

For all the reasons stated above, this Court should grant rehearing en banc.

Respectfully submitted,

MICHAEL W. PRICE
National Association of Criminal
Defense Lawyers

GEREMY C. KAMENS
Federal Public Defender

s/ Michael W. Price
Litigation Director, Fourth
Amendment Center
1660 L Street NW, 12th Floor
Washington, DC 20036
(202) 465-7615
mprice@nacdl.org

s/ Laura J. Koenig
Laura J. Koenig
Assistant Federal Public Defender
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800
laura_koenig@fd.org

Dated August 22, 2024

REQUEST FOR REBRIEFING

If the Court grants rehearing, Mr. Chatrue respectfully requests the opportunity for rebriefing. Mr. Chatrue’s opening brief focused on the issue that he lost (good faith), not on whether there is a Fourth Amendment interest in Location History, which the

district court assumed. J.A. 1368. Although addressed at length in his reply, *see* ECF 48 at 11-13, the panel refused to consider Mr. Chatrie's property interest in his Location History. Op.23 n.20. Mr. Chatrie therefore asks this Court to order rebriefing should it grant this petition.

CERTIFICATE OF COMPLIANCE

1. This petition for rehearing en banc has been prepared using Word for Office 365 software, Times New Roman font, 14-point proportional type size.
2. The body of this petition, exclusive of the case caption, title, and signature block, contains no more than 3,900 words, specifically 3,897 words.

I understand that a material misrepresentation can result in the Court's striking the brief and imposing sanctions. If the Court so requests, I will provide an electronic version of the brief and/or a copy of the word or line print-out.

August 22, 2024

Date

s/ Laura J. Koenig

Laura J. Koenig

Assistant Federal Public Defender