No. ____

IN THE
Supreme Court of the United States

OKELLO CHATRIE,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Petition for a Writ of Certiorari
to the United States Court of Appeals
for the Fourth Circuit

PETITION FOR A WRIT OF CERTIORARI

GEREMY C. KAMENS
Federal Public Defender
LAURA J. KOENIG
Assistant Federal Public Defender
PATRICK BRYANT
Assistant Federal Public Defender
OFFICE OF THE FEDERAL PUBLIC DEFENDER,
EASTERN DISTRICT OF VIRGINIA
1650 King Street,
Suite 500
Alexandria, VA 22314
(703) 600-0800

ADAM G. UNIKOWSKY
Counsel of Record
LAUREL A. RAYMOND
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
AUnikowsky@jenner.com

QUESTION PRESENTED

This case concerns the constitutionality of geofence warrants. For cell phone users to use certain services, their cell phones must continuously transmit their exact locations to their service providers. A geofence warrant allows law enforcement to obtain, from the service provider, the identities of users who were in the vicinity of a particular location at a particular time.

In this case, law enforcement obtained, and served on Google, a geofence warrant seeking anonymized location data for every device within 150 meters of the location of a bank robbery within one hour of the robbery. After Google returned an initial list, law enforcement sought—without seeking an additional warrant—information about the movements of certain devices for a longer, two-hour period, and Google complied with that request as well. Then—again without seeking an additional warrant—law enforcement requested de-anonymized subscriber information for three devices. One of those devices belonged to petitioner Okello Chatrie. Based on the evidence derived from the geofence warrant, petitioner was convicted of armed robbery.

The questions presented are:

1. Whether the execution of the geofence warrant violated the Fourth Amendment.

2. Whether the exclusionary rule should apply to the evidence derived from the geofence warrant.

RELATED PROCEEDINGS

This case arises from and is related to the following proceedings in the United States District Court for the Eastern District of Virginia and the United States Court of Appeals for the Fourth Circuit:

- *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. 2022).

- *United States v. Chatrie*, 107 F. 4th 319 (4th Cir. 2024) (panel opinion)

- *United States v. Chatrie*, 2024 WL 4648102 (4th Cir. 2025) (granting rehearing en banc)

- *United States v. Chatrie*, 136 F. 4th 100 (4th Cir. 2025) (en banc opinion)

TABLE OF CONTENTS

TABLE OF APPENDICES

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS AND STATUTES

OTHER AUTHORITIES

PETITION FOR A WRIT OF CERTIORARI

Petitioner Okello Chatrie respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Fourth Circuit.

OPINIONS BELOW

The Fourth Circuit's en banc opinion is reported at 136 F.4th 100 (4th Cir. 2025). Pet. App. 1a. The Fourth Circuit's initial opinion is reported at 107 F.4th 319 (4th Cir. 2024). Pet. App. 145a. The district court's opinion denying suppression is reported at 590 F. Supp. 3d 901 (E.D. Va. 2022). Pet. App. 264a.

JURISDICTION

The Fourth Circuit issued its decision on April 30, 2025. This Court has jurisdiction under 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL PROVISION

The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

INTRODUCTION

This case presents important constitutional questions concerning the controversial law enforcement tool known as the "geofence warrant."

Many cell phone owners use services that continuously transmit their exact location to their

service providers. Service providers use this information to track users' location over time. Based on this information, service providers can identify all users who were in a particular geographic area at a given time.

That capability has given rise to the geofence warrant. Geofence warrants seek information regarding devices that were within a particular geographic area during a particular time period. The warrant draws a virtual "fence" around a particular geographic area (hence "geofence") and seeks information about devices within that "fence" during the relevant time period.

This case involves a geofence warrant served on Google. Every two minutes, Google's Location History service records the user's location. The geofence warrant in this case directed Google to scan through the private user-controlled accounts of over 500 million Location History users to identify all devices that were, within one hour of a bank robbery, within 150 meters from the scene of the crime. After Google complied with that request, law enforcement sought and received additional location information for certain devices whose movements law enforcement deemed suspicious. Finally, without obtaining an additional search warrant, law enforcement requested and received names associated with three devices—which included petitioner Okello Chatrie. Petitioner was charged with, and convicted of, bank robbery.

Geofence warrants are a powerful law enforcement tool. At the same time, they raise significant Fourth Amendment concerns. This Court has been attuned to the privacy risks of new law enforcement techniques involving cell phones: In *Carpenter v. United States*, 585

U.S. 296 (2018), this Court held that cell phone users retain a reasonable expectation of privacy in the record of their physical movements as captured by cell-site location information (CSLI), through which cell providers can triangulate and track cell phone users' location. *Id.* at 309-10. The privacy concerns arising from geofence warrants are even greater than the privacy concerns at issue in *Carpenter*. In *Carpenter*, law enforcement officials sought information about the movements of a single individual suspected of a crime based on the movements of his cell phone. By contrast, using a geofence warrant, law enforcement may request information regarding *all* people who were at a sensitive location—an abortion clinic, a protest, a political party's convention—at a particular time.

It would be an understatement to say that lower-court judges have disagreed on the constitutional questions arising from geofence warrants. The Fourth Circuit panel in this case held that obtaining location information from Google was not a search at all. On rehearing en banc, the Fourth Circuit fractured, issuing a one-sentence per curiam affirmance accompanied by nine separate opinions.

The Fifth Circuit, meanwhile, has held both that requiring Google to search through over 500 million user accounts for responsive location information is a search, and that geofence warrants are unconstitutional general warrants, effectively banning geofence warrants in federal courts within the Fifth Circuit. The Texas Court of Criminal Appeals has rejected the Fifth Circuit's view—leading to a split between state courts and federal

courts in the same jurisdiction—as has the Georgia Supreme Court.

The uncertainty over geofence warrants is intolerable. When magistrate judges receive requests for geofence warrants, they need to know what rules apply. The same is true for tech companies that wish to cooperate with law enforcement while also protecting their users' privacy and complying with the Constitution. Although Google announced plans to change its internal policies such that it no longer stores location information on its central servers, the state of those plans and the status of its existing data are both unclear, and geofence warrants have been served on other companies as well, including Apple, Lyft, Snapchat, and Uber. This issue is not going away. This Court's review is needed.

On the merits, this Court should hold that the geofence warrant violated petitioner's Fourth Amendment rights. To begin, as Judge Wynn and Judge Berner's opinions below explain in detail, *Carpenter* dictates the conclusion that the government conducted a search. The *Carpenter* Court held that the collection of CSLI was a search because cell phone users have a reasonable expectation of privacy in CSLI, and every aspect of the Court's reasoning in *Carpenter* applies with equal or greater force here. Location History data is more comprehensive than the CSLI at issue in *Carpenter*; Location History allows for surveillance of everyone in a particular "fence," rather than just one person; Location History, like CSLI, allows access to intimate information about a person's life; and, as with

CSLI, obtaining Location History is easy and inexpensive for law enforcement.

In *Carpenter*, Justice Gorsuch stated that the Fourth Amendment analysis should turn not on whether a person has a reasonable expectation of privacy, but instead on whether he has a property interest in the item searched. Applying that approach here leads to the same result. Unlike CSLI, Location History is not a business record. Instead, Location History belongs to the user—the user can delete it or direct Google to stop collecting it. In this case, by collecting information that belonged to petitioner, law enforcement conducted a search.

Although the government obtained a geofence warrant, that warrant was inadequate to justify the search. As the Fifth Circuit has held, geofence warrants do not satisfy the Fourth Amendment's particularity requirement. Even assuming, contrary to the Fifth Circuit's view, that geofence warrants are sometimes constitutional, the execution of the warrant violated the Fourth Amendment here. The government should have obtained a warrant *after* Google returned its list. Obtaining a warrant at the first step was insufficient under the Fourth Amendment to justify the government's winnowing process and ultimate unmasking of petitioner's identity without further court review.

The Court should therefore grant certiorari on the first question presented and hold that the execution of the geofence warrant violated the Fourth Amendment.

The Court should also grant review on the second question presented: whether the exclusionary rule applies.

In the Fourth Circuit, every judge other than Judge Gregory concluded either that there was no Fourth Amendment violation or that the good-faith exception to the exclusionary rule applied. Petitioner agrees with Judge Gregory's assessment that the good-faith exception does not apply because the officers' conduct was not objectively reasonable. Further, the good-faith exception should not apply where, as here, the warrant at issue is a general warrant that authorizes the search of millions of accounts without probable cause.

Additionally, there is a more fundamental reason to reject the good-faith exception in this case. If the Court applies the good-faith exception, it will be impossible for this Court to issue an opinion deciding the constitutionality of geofence warrants (or any other novel surveillance tool) that will benefit the litigant. In every civil case, the officer will be protected by qualified immunity. In every criminal case, the defendant's conviction will stand regardless of the warrant's constitutionality. The result will be that confusion and lower-court splits will persist forever.

This Court has left open the possibility that it would not apply the exclusionary rule in cases where the good-faith exception would stunt the development of the law. That is this case. The Court should hold that the wrongfully-obtained evidence cannot be used against petitioner and reverse petitioner's conviction.

STATEMENT OF THE CASE

A. Geofence Warrants

The geofence warrant in this case was directed at Google and relied on a Google feature called "Location History." Pet. App. 270a. Location History draws from GPS information, Bluetooth beacons, CSLI, IP address information, and nearby Wi-Fi networks to log a device's location, making a record, on average, every two minutes. Pet. App. 271a. It is powerful enough to determine if a person is on the "second [or first] floor of [a] mall," and can determine a person's location to within as little as three meters. Pet. App. 272a, 274a.

Location History is not automatically enabled. However, Google offers multiple methods to turn Location History on and typically prompts users to do so multiple times across multiple apps, starting from when a user first sets up her Google account. Pet. App. 273a. If a user does not enable Location History immediately upon account setup, Google will prompt her to do so when she sets up an app with "Location History-powered features," like Google Maps, Google Photos, and Google Assistant, telling her it is necessary to "[g]et the most from" the app. Pet. App. 279a (brackets omitted). And once a user enables Location History through one app, it is enabled across all of her Google devices, and it will continue to be active even if she deletes the original app. Pet. App. 273a. Google collects and stores Location History at all times, regardless of whether the user is actively using her phone.

After opting in, a user can "pause" the collection of her data, though if she does so, a pop-up screen will warn her that pausing Location History will "limit[]

functionality of some Google products over time." Pet. App. 282a (bracket in original). Pausing Location History does not delete previously-collected data—it merely pauses collection of new data. Pet. App. 283a. If a user wanted to delete her location history in 2018—when petitioner first (seemingly inadvertently) enabled his Location History—there was only one way to do so: by visiting myactivity.google.com. Pet. App. 281a, 283a, 333a. One Google employee remarked that the user interface "*feels* like it is designed to make things *possible*, yet *difficult* enough that people won't figure…out" how to turn Location History off—a sentiment the district court endorsed. Pet. App. 283a-284a.

Because Google produces both Android phones and apps like Google Maps that function across devices, Google is able to collect detailed location data, including Location History, on "numerous tens of millions" of users. Pet. App. 270a; *see also* Pet. App. 272a n.8. At the time the warrant in this case was executed, Google stored this extensive data in a repository known as the "Sensorvault," where each datapoint is associated with a unique device ID. Pet. App. 272a. Google uses this data for advertising and to power models and support features of Google apps, such as maps. Pet. App. 272a. While the default storage method is anonymized, Google can also de-anonymize the information to reconstruct the movements of a particular user. Even without explicit de-anonymization, the granularity of the data is such that, in many cases, a few data points, used in conjunction with other publicly available information, can be used to unmask a user's likely identity. *See* Pet. App. 305a.

Geofence warrants rely on this vast trove of data. When law enforcement serves a geofence warrant on Google, it identifies a geographic area—the geofence—which is typically a circle with a specified radius. Pet. App. 285a. Then it identifies a certain span of time, and requests Location History data for all users within that area during that time. Pet. App. 285a. Law enforcement's early geofence requests were broad, asking Google to produce account-identified information of all users caught in the geofence. Pet. App. 286a. Concerned by the threat these requests posed to user privacy, Google developed its own three-step response process.

First, law enforcement must obtain a warrant compelling Google to disclose a "de-identified" list of all Google users whose Location History indicates they were in the geofence at any point during the specific time. Pet. App. 286a. Then, to create the list required by the warrant, Google searches all Location History user accounts in the Sensorvault for users whose stored Location History indicates their location was somewhere in the geofence. Pet. App. 287a. Google then compiles a list for law enforcement including, for each user, the stored latitude/longitude coordinates and timestamp, the confidence interval (Google's estimate of how accurate the location data is), and the source of the Location History (i.e., whether it came from Wi-Fi, GPS, or cell tower). Pet. App. 287a-288a. At this step, each user's information is connected to a "de-identified" unique device account number, rather than an email or name. Pet. App. 287a.

Second, the government reviews the list of de-identified data. If needed, it may then ask Google for the Location History of the users identified in step one for a longer period of time than the original geofence, without the geographic barrier. Pet. App. 289a-290a. This gives the government a more complete picture of the relevant users' movements. Typically, Google requires the government to narrow its request to a subset of accounts from the original geofence. Pet. App. 290a.

Third and finally, the government compels Google to provide the names and account identifiers—either email addresses or phone numbers—associated with particular devices it analyzed at step two. Thus, for those users, the government obtains a complete and granularly detailed record of their movements, associated with their names and email addresses. While Google prefers that law enforcement winnow down the accounts it analyzed at step two, it is "possible" that Google would provide account-identified location data for all users in step two. Pet. App. 290a-291a.

In December 2023, Google announced that it would begin saving users' Location History on their devices, rather than in the Sensorvault repository. *See* Letter from Appellant under Fed. R. App. P. 28(j) (4th Cir. Dec. 20, 2023), Dkt. No. 62. Though Google announced that it intended to make this change gradually over the year between 2023 and 2024, petitioner is not aware of any subsequent announcements that the change has been made, detailing how the change affects legacy Google devices, or specifying which data Google continues to collect. Geofence warrants continue to be litigated. *See e.g.* Stipulation Order to Partially Unseal Records in

Sealed Case, *In re Google*, Case No. 25-mj-70146 (N.D. Cal. Feb. 7, 2025), ECF No. 1, Exhibit A (motion to quash geofence warrant filed on February 7, 2024).

B. Factual Background

On May 20, 2019, someone robbed the Call Federal Credit Union in Midlothian, Virginia. Pet. App. 265a-266a. Upon entering the bank, the suspect handed the teller a note demanding $100,000. Pet. App. 291a; 266a. He then forced the manager to open the vault at gunpoint, took $195,000 in cash, and left the bank on foot. Pet. App. 266a-267a. Detective Hylton of the local police responded to the scene, interviewed witnesses, and reviewed surveillance video. Pet. App. 291a. After unsuccessfully pursuing other leads, on June 14, 2019, Detective Hylton applied for and obtained a geofence warrant, ultimately leading to petitioner's arrest. Pet. App. 292-293a.

Detective Hylton followed Google's three-step procedure. He presented a magistrate judge with a warrant for a geofence with a 300-meter diameter—longer than three football fields—drawn over the site of the robbery, encompassing a swath of urban Midlothian and including both the bank and a nearby church. Pet. App. 294a. At step one, the warrant called for de-identified information for all user accounts inside the geographical area from 4:20 pm to 5:20 pm. Pet. App. 295a. For step two, it expanded the time frame from 3:50 to 5:50 and lifted the geographic limits. Pet. App. 296a. And at step three, the warrant called for the accounts to be linked to specific, identifiable users. Pet. App. 296a-297a. In the warrant's accompanying affidavit, Detective Hylton stated that the perpetrator appeared to be using

a cell phone in the surveillance footage, and that "when people act in concert with one another to commit a crime, they frequently utilize cellular telephones." Pet. App. 296a. The magistrate judge signed it, and Detective Hylton sent it to Google on June 20, 2019. Pet. App. 298a.

Google executed step one of the geofence and provided Detective Hylton with anonymized data for nineteen users caught within the geofence. Pet. App. 299a. Detective Hylton subsequently requested additional location data on nine users, which Google provided. Detective Hylton did not explain to Google why he chose these nine accounts, nor did he consult a magistrate. Pet. App. 299a-300a. Finally, Detective Hylton requested that Google de-anonymize three of the numbers, again without explaining why or consulting a judge. Pet. App. 300a. Google provided the information. Pet. App. 300a.

Ultimately, the geofence warrant led law enforcement to petitioner, who was indicted on charges of Forced Accompaniment During Armed Bank Robbery, 18 U.S.C. § 2113(a), (d), and (e), and Using, Carrying, or Brandishing a Firearm During and in Relation to a Crime of Violence. 18 U.S.C. § 924(c)(1)(A).

C. District Court Proceedings

Petitioner moved to suppress the fruits of the geofence warrant. The district court conducted extensive fact-finding, relying on, among other things, an amicus brief by Google, four declarations by Google employees, and in-person testimony from Google employees. Pet. App. 306a-308a. In the end, the district court concluded that the warrant violated the Fourth

Amendment because the government lacked "any semblance of … particularized probable cause" to search every one of the nineteen users swept into the geofence. Pet. App. 312a. It further concluded that steps two and three—undertaken with no judicial oversight—"improperly provided law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions," and independently failed the Fourth Amendment's particularity requirement. Pet. App. 313a.

The court rejected the government's argument that petitioner forfeited his Fourth Amendment rights by providing his Location History to Google. It concluded that under *Carpenter*, "a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting 'YES, I'M IN' at midnight," and that Google's warnings were insufficient to provide for voluntary consent. Pet. App. 333a. Finally, the court noted that geofence warrants intrude into the private lives of many Americans who may never have a chance to contest the incursion. Pet. App. 310a. Nonetheless, the district court declined to suppress the evidence through application of the good-faith exception to the exclusionary rule. *See United States v. Leon*, 468 U.S. 897, 923 (1984).

Petitioner entered a conditional guilty plea, reserving his right to appeal the denial of his motion to suppress. Pet. App. 80a. He was sentenced to 141 months' imprisonment. *Id.*

D. Fourth Circuit Proceedings.

A divided Fourth Circuit panel affirmed on different grounds. In the majority, Judges Richardson and

Wilkinson concluded that no search occurred, because petitioner voluntarily exposed his information to Google. Pet. App. 148a. Dissenting, Judge Wynn concluded that under *Carpenter*, the geofence warrant here resulted in a Fourth Amendment search. Pet. App. 187a.

The Fourth Circuit reheard the case en banc and affirmed in a one-sentence per curiam opinion without any reasoning. Pet. App. 4a. The court divided 7-7 on whether a Fourth Amendment search had occurred, with one judge declining to reach the issue. Of the seven judges who found a Fourth Amendment search, however, six concluded that the evidence should not be suppressed under the good-faith exception to the exclusionary rule, with Judge Gregory dissenting. Nine judges wrote separate opinions airing "widely divergent views." Pet. App. 5a.

Seven judges—Judges Wilkinson, Niemeyer, King, Agee, Richardson, Quattlebaum, and Rushing—found that there was no Fourth Amendment search. Four wrote separately.

Judge Richardson, joined by Judges Wilkinson, Niemeyer, King, Agee, Quattlebaum, and Rushing, concluded that no Fourth Amendment search occurred, and therefore no warrant was necessary. Pet. App. 81a. According to Judge Richardson, petitioner "did not have a reasonable expectation of privacy in two hours' worth of Location History data voluntarily exposed to Google." Pet. App. 80a-81a. Judge Richardson distinguished *Carpenter* on two grounds: first, *Carpenter* did not apply to a request for only two hours of data, which he characterized as encompassing only a "single, brief trip," and second, *Carpenter* did not apply to Location History

because users "knowingly and voluntarily" expose this data to Google. Pet. App. 92a; 93a.

Judge Wilkinson, joined by Judges Niemeyer, King, Agee, and Richardson, concluded that no search occurred under the third-party doctrine, arguing that the case involved a "straightforward" application of *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States. v. Miller*, 425 U.S. 435 (1976). Pet. App. 23a. He urged that treating collection of Location History as a search would allow "tech-savvy criminals" to commit crimes without consequence. Pet. App. 25a.

Judge Niemeyer opined that collecting Location History is akin to collecting "markers" from the public place of a crime. In Judge Niemeyer's view, just as police officers may collect boot prints, tire tracks, left-behind items or DNA from a crime scene, so too may they collect Location History through a geofence. Pet. App. 33a.

Judge King noted his concurrence with Judges Wilkinson and Richardson, and also stated that he would affirm based on the good-faith exception. Pet. App. 36a.

Seven judges—Judges Gregory, Wynn, Thacker, Harris, Heytens, Benjamin, and Berner—concluded that a Fourth Amendment search had occurred. Two of those judges (Judges Harris and Heytens) stopped there and concluded that the good-faith exception to the exclusionary rule applied; four judges (Judges Wynn, Thacker, Benjamin, and Berner) went on to find that the Fourth Amendment was violated, but also found the good-faith exception applicable; and one judge (Judge Gregory) would have excluded the evidence and reversed petitioner's conviction.

Judge Wynn, joined by Judges Thacker, Harris, Benjamin, and Berner (in full) and by Judge Gregory (except as to the good-faith exception), concluded that a Fourth Amendment search had occurred under *Carpenter*. He emphasized that in light of the "frictionless" nature of enabling Location History as well as its "comprehensive, retrospective, intimate, and highly efficient surveillance," the third-party doctrine was "wholly inadequate" to obviate petitioner's reasonable expectation of privacy in his Location History data. Pet. App. 69a. Judge Wynn characterized the en banc court as "squander[ing]" "a critical opportunity to clarify the Fourth Amendment's application to emerging surveillance technologies." Pet. App. 38a. In declining to decide, Judge Wynn cautioned, the court not only "clear[ed] the path for widespread, surreptitious police surveillance," but also fell "short of [its] duty." Pet. App. 70a-71a. He concluded, however, that the evidence should not be excluded under the good-faith exception to the exclusionary rule. Pet. App. 38a.

Judge Berner, joined by Judges Gregory, Wynn, Thacker, and Benjamin, and in part by Judge Heytens, similarly concluded that a search occurred. Judge Berner interpreted *Carpenter* to lay out two factors governing whether one holds a reasonable expectation of privacy in information given to a third party: "(1) how revealing that data is, and (2) whether the information was, in practical terms, given to the third party voluntarily." Pet. App. 111a. She concluded that under *Carpenter*, law enforcement conducts a search when it obtains "any amount" of "non-anonymous" Location History. Pet. App. 111a-112a. Judge Berner noted that at Google's first step, the warrant required only one

hour of information gleaned from primarily public streets. Pet. App. 115a. Because of the request's short duration, limited geofence size, and coverage of only public areas, she concluded that the data revealed in step one was unlikely to be traceable to any specific individual. Pet. App. 115a. At step two, however, the government requested, and Google provided, non-geographically limited data from a longer period of time, which likely would—and did—show users entering homes and offices. Pet. App. 101a. The step two data, then "was not truly anonymous." *Id.* And at step three, the data became explicitly non-anonymous, because the government asked Google to reveal the names, email addresses, and phone numbers associated with the relevant Google users. *Id.* Steps two and three, Judge Berner determined, infringed petitioner's reasonable expectation of privacy. Pet. App. 121a-122a, 125a.

In a portion of her opinion not joined by Judge Heytens, Judge Berner concluded that the search violated the Fourth Amendment because the government lacked probable cause to search any specific Google user at the time it applied for the warrant. Pet. App. 126a. She emphasized that "[b]ecause the detective could not explain why he would eventually search the Location History data of certain, then-unknown users in Google's dataset, he failed to show probable cause to conduct the second and third requests." Pet. App. 126a. "Under the terms of the geofence warrant, Google, not a magistrate, was the sole entity that could confine the scope of the ultimate search." Pet. App. 126a. "Probable cause determinations cannot be delegated to private entities." Pet. App. 126a. Judge Berner disagreed, however, with

the Fifth Circuit's view that geofence warrants are always unconstitutional. Pet. App. 126a.

Judge Heytens, joined by Judges Harris and Berner, wrote that regardless of whether a Fourth Amendment violation occurred, exclusion of the evidence was unwarranted because first, "the legal landscape was uncertain when this investigation happened," and second, Detective Hylton sought the advice of prosecutors and obtained a warrant. Pet. App. 98a.

Judge Gregory dissented from the per curiam opinion. He concluded that the Fourth Amendment was violated, the good-faith exception should not apply, and the evidence should be suppressed. Judge Gregory noted that though Detective Hylton obtained a warrant, "[e]ven now, the government cannot tell us what justified the more intrusive searches at [s]tep [t]wo or [t]hree, or how or why there was probable cause to search those individuals," leaving it with "unbridled discretion." Pet. App. 133a, 135a. In Judge Gregory's view, to hold that lack of judicial guidance as to a specific measure immunized it from exclusion "would run the risk of forgiving law enforcement impropriety simply because no court has specifically forbidden it," rendering Fourth Amendment protections "a nullity in the face of rapidly emerging technology." Pet. App. 139a.

Finally, **Chief Judge Diaz**, unlike his 14 colleagues, declined to decide whether a search had occurred. Instead, he voted to affirm the district court's decision solely through application of the good-faith exception. Pet. App. 5a. He noted the divergence among his colleagues: "[o]ne camp insists that disallowing geofence warrants would contravene our precedent, hamstring

law enforcement…and chill innovation," while the other "is just as adamant that granting blanket approval to these warrants would contravene our precedent and compromise the privacy interests of cell phone users." Pet. App. 14a. But in light of the "shallow well of…legal authority," Judge Diaz chose to "wait." Pet. App. 14a.

REASONS FOR GRANTING THE PETITION

I. LOWER COURTS ARE DIVIDED ON THE CONSTITUTIONALITY OF GEOFENCE WARRANTS.

The Fourth Circuit's judges were intractably divided over the application of the Fourth Amendment to geofence warrants. That internal disagreement parallels the disagreement among other courts.

To begin, a unanimous **Fifth Circuit** panel—in conflict with the views of judges on both sides of the Fourth Circuit's divide—concluded that geofence warrants always violate the Fourth Amendment. *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024), *petition for cert. filed*, No. 24-7237 (U.S. May 19, 2025).

The Fifth Circuit first held that collecting Location History is a Fourth Amendment search. In the Fifth Circuit's view, "[g]iven the intrusiveness and ubiquity," Google users have a reasonable expectation of privacy in their Location History data. *Id.* at 836. The court concluded that the third-party doctrine did not apply under a "straightforward" application of *Carpenter*. *Id.* at 835.

The Fifth Circuit further held that geofence warrants are unconstitutional because they violate the Fourth Amendment's particularity requirement. It

explained that geofence warrants are a modern incarnation of the "reviled 'general warrants' and 'writs of assistance' of the colonial era." *Id.* at 836. General warrants specify an offense but allow officers the discretion to determine which persons to arrest and which places to search. *Id.* The Fifth Circuit drew a parallel to the first step of Google's geofence response protocol, which is to search the entire Sensorvault database—all 592 million individual accounts—for users who were at a particular location at a given moment, even though law enforcement does not yet know—and may never know—who they are looking for. *Id.* at 837. Accordingly, the Fifth Circuit held that "geofence warrants fail at Step-1—they allow law enforcement to rummage through troves of location data from hundreds of millions of Google users without any description of the particular suspect or suspects to be found." *Id.* at 837-38. The court held, however, that the evidence should not be suppressed under the good-faith exception to the exclusionary rule. *Id.* at 839.

The **Texas Court of Criminal Appeals** has rejected the Fifth Circuit's reasoning in *Smith*, resulting in a conflict of authority between federal and state courts in the same jurisdiction. In *Wells v. State*, No. PD 0669-23, -- S.W.3d --, 2025 WL 980996 (Tex. Crim. App. Apr. 2, 2025), the court considered the constitutionality of a warrant that followed Google's three-step process. Like the Fourth Circuit, the Texas Court of Criminal Appeals fractured badly. Although no single opinion attracted a majority of the court, eight of the nine Justices agreed that steps one and two of Google's three-step process satisfied the Constitution, thus rejecting the Fifth Circuit's approach. *See id.* at *10 (opinion of Yeary, J.)

(declining to decide whether search occurred but finding that warrant was supported by probable cause and was sufficiently particularized); *id.* at *13 (opinion of Finley, J.) (finding no search); *id.* at *16 (opinion of Newell, J.) (finding no search).

As for step three, the Justices could not agree on the appropriate disposition, with four Justices voting to affirm the conviction based on varying rationales, *id.* at *10 (opinion of Yeary, J.); *id.* at *13 (opinion of Finley, J.), four Justices voting to vacate, *id.* at *18 (opinion of Newell J.), and one Justice, Justice McClure, dissenting without opinion.

The **Georgia Supreme Court** has similarly rejected the Fifth Circuit's *Smith* decision. In *Jones v. State*, 913 S.E.2d 700 (Ga. 2025), the court upheld the constitutionality of a geofence warrant directed to Google. The court did not decide whether a search had occurred, *id.* at 706 n.1, instead holding that the warrant satisfied the Fourth Amendment's probable cause and particularity requirements. The court concluded that the geofence warrant was supported by probable cause as to steps 1 and 2. *Id.* at 707. Contrary to the Fifth Circuit, the Georgia Supreme Court determined that "the description of the search in steps one and two of the first warrant was not the kind that raises the specter of a general rummaging, and it thus satisfies the particularity requirement." *Id.* at 711. Unlike in this case, law enforcement in *Jones* obtained a second search warrant at step three, and the court held that the second search warrant was supported by probable cause. *Id.* at 708.

The **Colorado Supreme Court**, addressing a slightly different issue, has also reached a conclusion inconsistent with the Fifth Circuit. In *People v. Seymour*, 536 P.3d 1260 (Colo. 2023), the Colorado Supreme Court addressed the constitutionality of a reverse keyword warrant, which required Google to identify users who had done a particular search within a particular period. Contrary to the Fifth Circuit, the court held that the reverse keyword warrant was not a general warrant and did not violate the Fourth Amendment's particularity requirement. *Id.* at 1276. It reasoned that "a search isn't unconstitutional simply because the government, in some lightning-fast, digital sense, very cursorily examines unrelated documents … [s]uch brief examination doesn't turn an adequately particularized search warrant into an unconstitutional general warrant." *Id.* The court ultimately did not resolve the defendant's other Fourth Amendment objections and instead affirmed based on the good-faith exception to the exclusionary rule. *Id.* at 1278.

Three members of the court would have held, like the Fifth Circuit, that a warrant directing Google to search through all accounts was an unconstitutional general warrant. Justice Berkenkotter concurred based on the good-faith exception but "strongly disagree[d] with the majority's conclusion that the examination of a billion Google users' search histories was not unreasonably intrusive because the government didn't ultimately seize all of those search histories." *Id.* at 1281 (Berkenkotter, J., concurring). The dissenting Justices likewise concluded that "by authorizing law enforcement to rummage through the private search histories of a billion individuals for potential evidence of criminal

activity, reverse-keyword warrants permit exactly what the Fourth Amendment forbids. They are tantamount to a high-tech version of the reviled 'general warrants' that first gave rise to the protections in the Fourth Amendment." *Id.* at 1282 (Marquez, J., dissenting).

II. THIS CASE WARRANTS SUPREME COURT REVIEW.

The Court should grant certiorari in this case. The question presented is profoundly important, the confusion in lower courts is intolerable, and this case is an appropriate vehicle given the well-developed facts and well-preserved legal arguments.

A. The Issue is Important.

The question presented is both practically and jurisprudentially important.

In recent years, law enforcement use of geofence warrants has skyrocketed. Google received its first geofence warrant in 2016. Pet. App. 285a. From 2017 to 2018, Google experienced a 1,500% increase in requests. Pet. App. 285a. By 2021, geofence warrants constituted 25% of all warrants submitted to Google. Pet. App. 285a. Geofence warrants have been used to investigate crimes ranging from smashed windows to the storming of the Capitol. *United States v. Rhine*, 652 F. Supp. 3d 38, 46 (D.D.C. 2023).

This fundamental new law enforcement tool has attracted widespread attention. Numerous Fourth

Amendment scholars have analyzed the issue,[1] with a leading Fourth Amendment scholar observing that the decision below yields "a crazy amount of uncertainty."[2] Given the ubiquity of location-tracking services, geofence warrants have also resulted in substantial public commentary.[3]

---

[1] *See e.g.* Brian L. Owsley, *The Best Offense Is A Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 Hofstra L. Rev. 829, 834 (2022); Haley Amster & Brett Diehl, Note, *Against Geofences*, 74 Stan. L. Rev. 385, 389 & n.11 (2022); Note, *Geofence Warrants and the Fourth Amendmen*t, 134 Harv. L. Rev. 2508, 2512 (2021); A. Reed McLeod, Note, *Geofence Warrants: Geolocating the Fourth Amendment*, 30 Wm. & Mary Bill Rts. J. 531, 532 (2021); Orin S. Kerr, *Data Scanning and the Fourth Amendment* (Stan. Pub. L., Working Paper, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5175686; Orin Kerr, *The Fifth Circuit Shuts Down Geofence Warrants—and Maybe A Lot More*, Lawfare (Aug. 14, 2024), https://www.lawfaremedia.org/article/the-fifth-circuit-shuts-down-geofence-warrants-and-maybe-a-lot-more; Jackie O'Niel, *Much Ado About Geofence Warrants*, Harv. L. Rev. Blog. (Feb. 18, 2025), https://harvardlawreview.org/blog/2025/02/much-ado-about-geofence-warrants/.

[2] Orin S. Kerr, *The Fourth Circuit's Geofencing Case Ends Not With a Bang But A Whimper*, reason (May 2, 2025), https://reason.com/volokh/2025/05/02/the-fourth-circuits-geofencing-case-ends-not-with-a-bang-but-a-whimper/.

[3] *See e.g.* Andrew Couts, *Security News This Week: Geofence Warrants Ruled Unconstitutional—but That's Not the End of it*, WIRED (Aug. 17, 2024), https://www.wired.com/story/geofence-warrants-ruled-unconstitutional-tmobile-fine-deepfake-nudes-lawsuit/; Shira Ovide, *Police Love Google's Surveillance Data: Here's How to Protect Yourself*, Wash. Post (Oct. 24, 2023), https://www.washingtonpost.com/technology/2023/10/24/google-privacy-police-geofence/; Sidney Fussell, *An Explosion in Geofence Warrants Threatens Privacy Across the U.S.*, Wired (Aug. 27,

Yet tech companies and magistrate judges have been forced to grapple with these difficult and consequential questions on their own. Tech companies have had no choice but to develop protocols, without judicial guidance, for balancing law enforcement interests with user privacy. The three-step procedure in this case was designed by Google. This Court—not a private business—should decide how the Fourth Amendment works in the context of geofence warrants.

What is more, magistrate judges must reinvent the wheel every time they are faced with a geofence warrant. For ordinary warrants, a magistrate judge's duties are well-understood. The magistrate judge must assess whether there is probable cause and the warrant is sufficiently particularized—tasks magistrate judges accomplish every day.

Geofence warrants, by contrast, are a fundamentally new and different type of warrant, forcing magistrate judges to engage in first-principles constitutional analysis. And that analysis has not proved easy. As catalogued above, judicial views of geofence warrants have spanned the gamut, ranging from the view of seven Fourth Circuit judges that geofence warrants are never needed because collection of location information is not a search, to the Fifth Circuit's view that geofence warrants result in the unconstitutional search of hundreds of millions of private user accounts every time they are executed. The Fourth Circuit and Texas Court

---

2021), https://www.wired.com/story/geofence-warrants-google/; Jennifer Valentino-deVries, *Tracking Phones, Google is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

of Criminal Appeals produced nearly as many intermediary positions as there are judges. Magistrate judges should not be forced to evaluate and pick one of these positions every time they receive a warrant application. It is incumbent on this Court to decide these fundamental constitutional questions.

Certiorari is warranted, too, in view of the privacy implications of geofence warrants. As this Court has recognized, cellphones are now so "pervasive and insistent" in modern life that to an extraterrestrial visitor, they might be mistaken for a "feature of human anatomy." *Riley v. California*, 573 U.S. 373, 385 (2014). Most Americans "compulsively" carry their phone at all times. *Carpenter*, 585 U.S. at 311. The record in this case reflects that there are 1.5 billion Google users, of which about one third—hundreds of millions—have enabled Location History. Pet. App. 274a. As with the CSLI this Court addressed in *Carpenter*, those phones' location-tracking capabilities produce a "deep repository of historical location information" of users' daily movements accessible with "just the click of a button" and at "practically no expense." *Carpenter*, 585 U.S. at 311-12. And just as in *Carpenter*, because this information is collected for nearly all users at all times, "police need not even know in advance whether they want to follow a particular individual, or when." *Id.* at 312. The resulting system of "near perfect surveillance" is as if the government had "attached an ankle monitor" to tens of millions of Americans. *Id.*

Under the Fifth Circuit's view of geofence warrants, the government rummages through every user's private location information every time it executes a geofence

warrant. If that holding is right, millions of Americans are having their privacy rights violated every day. Even if that holding is wrong, millions of Americans face the risk that their identities will be unmasked and movements revealed without any judicial involvement. If the Constitution permits that outcome, this Court should say so.

B. This Case Is an Appropriate Vehicle.

The Court is unlikely to find a better vehicle than this case to resolve the constitutionality of geofence warrants.

First, the Fourth Circuit's one-line per curiam affirmance leaves all issues on the table for this Court. The Court is free to resolve whichever issues it deems appropriate—whether a search occurred, whether the warrant was sufficiently particularized, whether there was probable cause, or anything else—and leave other issues for the Fourth Circuit on remand.

Second, petitioner preserved all available Fourth Amendment arguments, and those arguments were the subject of widespread debate in the 126 pages of Fourth Circuit opinions. As Judge Wynn observed, "[t]he constitutional question in this case has been fully briefed, argued and exhaustively debated—not only by the parties but by amici and members of this Court. And it is unclear what future case could better tee up the issue." Pet. App. 38a.

Of particular note, petitioner preserved the argument that he had a property right in Location History. In *Carpenter*, Justice Gorsuch suggested that the Fourth Amendment analysis may have turned on

whether users had a property interest in CSLI, but could not "help but conclude—reluctantly—that Mr. Carpenter forfeited perhaps his most promising line of argument." 585 U.S. at 406 (Gorsuch, J., dissenting). In this case, by contrast, in the district court, petitioner repeatedly briefed the issue that he had a property interest in CSLI. 4th Cir. J.A. 39-40; J.A. 83-85; J.A. 382-383; J.A. 1102; J.A. 1172-1173. The government expressly acknowledged that petitioner had preserved a property-based theory "rooted in Justice Gorsuch's solo dissent in *Carpenter*." J.A. 62. In the Fourth Circuit, petitioner similarly argued that "[r]egardless of the duration of the search or the significant privacy interests at stake, Location History data fits into a simpler scheme: the Fourth Amendment protects it because it belongs to the users who created it." 4th Cir. Reply Br. 11.

The factual record in this case is also unusually extensive. Google participated in the district court as an amicus, providing detailed information about the technology involved as well as its internal processes. *See* Dkt. No. 29, Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a 'Geofence' General Warrant, 2019 WL 8227162. A Google "Location History Manager" submitted three declarations, a Google "Legal Investigations Specialist" submitted another, and both testified live. Indeed, the Fifth Circuit in *Smith* often relied on the findings of the district court from *Chatrie* for its description of what Location History is, how precise it is, how it is enabled, Google's geofence warrant protocol, and the ubiquity of geofences. *See e.g.*, 110 F.4th at 823-25. In short, the Court is unlikely to see

another case in which both the facts and the law are so well-developed.

III. PETITIONER'S FOURTH AMENDMENT RIGHT WAS VIOLATED.

The Court should hold that the geofence warrant in this case violated the Fourth Amendment.

A. The Government Conducted a Search.

When the government directed Google to execute the geofence warrant, it conducted a search under both the *Carpenter* majority's reasonable-expectations-of-privacy approach and under a property-based approach.

First, the government violated petitioner's reasonable expectation of privacy. The Fourth Amendment protects individuals against "arbitrary invasions by governmental officials" into the sphere in which a person has a reasonable expectation of privacy. *Carpenter*, 585 U.S. at 303 (quoting *Camara v. Mun. Ct. of City & Cnty. of S.F.*, 387 U.S. 523, 528 (1967)). Accordingly, when an individual "seeks to preserve something as private," and his "expectation of privacy is one that society is prepared to recognize as reasonable," intrusion into that sphere is a search. *Id.* at 304 (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)).

The *Carpenter* Court concluded that cell phone users have a reasonable expectation of privacy in their CSLI, and the same reasoning establishes that they have a reasonable expectation of privacy in their Location History. The Court recognized that CSLI is data that a person would reasonably expect to keep private, as it tracks "nearly exactly the movements of [a cell phone's] owner," *id.* at 311, allows the police to access

"retrospective" data, *id.* at 312, provides an "intimate window into a person's life," *id.*, and is "easy, cheap, and efficient." *Id.* at 311.

As Judge Wynn and Judge Berner explained in detail, and as the Fifth Circuit explained in *Smith*, each of these characteristics of CSLI is just as true of Location History data. Pet. App. 62a; Pet. App. 118a; *Smith*, 110 F.4th at 832-33. Location History offers even more precise tracking than CSLI and provides a detailed map of all of a person's movements, including movement into the most intimate of spaces. *See Carpenter*, 585 U.S. at 311 (noting that a cell phone "faithfully follows its owner…into private residences, doctor's offices, political headquarters, and other" revealing locales). It is also easy and cheap to obtain.

Carpenter also establishes that petitioner did not waive the protections of the Fourth Amendment by transmitting his Location History to Google. In *Carpenter*, the Court rejected the government's proffer to treat CSLI as simply a "garden-variety request for information from a third-party witness." *Id.* at 313. First, CSLI was intimately revealing, unlike the pen register and bank records at issue in *Smith* and *Miller*, the foundational third-party cases. And second, cellphone users do not, in any "meaningful sense," opt in to "turning over a comprehensive dossier of [their] physical movements." *Id.* at 315.

Transmission of Location History to Google is not meaningfully voluntary. As Judge Wynn and the Fifth Circuit explained, enabling Location History is "frictionless by design" and difficult to undo. Pet. App. 65a; *see Smith*, 110 F.4th at 835. Meanwhile, Google's

privacy warnings are "limited" and "partially hidden," and at the very least, do not inform users that enabling the feature might result in the government's unfettered access to their every move. Pet. App. 66a, 332a; *Smith*, 110 F.4th at 835-36.

As a result, the execution of the geofence warrant resulted in a search. As the Fifth Circuit explained, at the first step, the government searched the accounts of *all* users by directing Google to assess whether those users were within the geofence. *See Smith*, 110 F.4th at 837-38 (geofence warrants "allow law enforcement to rummage through troves of location data from hundreds of millions of Google users without any description of the particular suspect or suspects to be found"). Although this search did not unmask any particular user's identity, it was still a search—just as the police conducts a search if it rummages through a person's desk, even if it does not know who owns the desk. At a minimum—in line with Judge Berner's conclusion—the government conducted a search when it obtained Chatrie's account-identified location information. Pet. App. 121a. Google's disclosure of non-anonymized information regarding petitioner's whereabouts violated petitioner's reasonable expectation of privacy.

Under a property-based approach, the government conducted a search because Location History belongs to users, not Google. Location History is their digital papers and effects, their personal "journal" stored in their accounts, just like their Gmail, Google Docs, or Google Photos. Google's privacy policy consistently refers to user data (including Location History) as "your information," which can be managed, exported, and even

deleted from Google's servers at "your" request. 4th Cir. J.A. 39. Unlike the CSLI at issue in *Carpenter*, Location History is in no sense a business record: users (not Google) have control over whether it is stored and can unilaterally delete it. Although the records were stored on Google's servers, Google was acting as a bailee rather than an owner. Having directed Google to screen and then turn over the contents of petitioners' property, the government conducted a search.

B. The Warrant Violated the Fourth Amendment.

Although the government obtained a geofence warrant before conducting the search, the warrant did not comply with the Fourth Amendment.

First, the warrant violated the Fourth Amendment's particularity requirement. To comply with the Fourth Amendment, warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend IV. As the Fifth Circuit's *Smith* decision explains, geofence warrants are not particularized. "[L]aw enforcement cannot obtain its requested location data unless Google searches through the entirety of its Sensorvault—all 592 million individual accounts—for *all* of their locations at a given point in time." 110 F.4th at 837. "Moreover, this search is occurring while law enforcement officials have *no idea* who they are looking for, or whether the search will even turn up a result." *Id.* "Indeed, the quintessential problem with these warrants is that they *never* include a specific user to be identified, only a temporal and geographic location where any given user *may* turn up post-search." *Id.*

Even if geofence warrants are not categorically unconstitutional, this warrant was. The district court opined that it may be possible to narrowly describe the circumference of a geofence that would be supported by probable cause for the limited, anonymous information it provides, from which "officers likely could use that narrow, anonymous information to develop probable cause particularized to specific users." Pet. App. 325a. But that is not what occurred here. Detective Hylton sought and obtained a geofence warrant covering an area of downtown Midlothian the size of three football fields, with a confidence interval reach even larger. Then, at step two, Detective Hylton offered no reasoning to justify a more intrusive search of nine of the nineteen—unlimited as to geographic area, and longer in time—nor did he present his request for a more intrusive search to a neutral judge or magistrate.

At the third step, when Detective Hylton directed Google to unmask the identities of three account holders, he conducted a warrantless search without probable cause. Detective Hylton lacked probable cause to investigate those three accounts: he offered no reasoning to Google as to why these three accounts were singled out. And even if Detective Hylton offered such reasoning, Google is not a magistrate judge. Detective Hylton should have obtained a search warrant, supported by probable cause, before determining the identities associated with the devices he found suspicious. Because he failed to do so, the search violated the Fourth Amendment.

IV. THE GOOD-FAITH EXCEPTION DOES NOT APPLY.

The first question—whether this geofence warrant violated the Fourth Amendment—alone justifies this Court's intervention. Because the Fourth Circuit resolved this case via an unreasoned per curiam affirmance, the Court has the option of granting certiorari on the first question, and then, if it finds that an unconstitutional search occurred, remanding for the Fourth Circuit to decide whether the good-faith exception applies. Although the Fourth Circuit judges have already opined on that issue in their separate opinions below, they may reconsider their reasoning in light of this Court's Fourth Amendment analysis. Further, deciding the Fourth Amendment merits issue will guide lower courts and law enforcement on this important constitutional issue.

Nevertheless, to ensure that petitioner obtains meaningful relief from a decision in his favor, petitioner respectfully urges the Court to grant certiorari as to the second question presented and hold that the good-faith exception to the exclusionary rule does not apply.

To begin, petitioner agrees with Judge Gregory's conclusion that the good faith exception does not apply because "Hylton could not have reasonably believed that the liberty authorized by the warrant was constitutional given the lack of specificity the Fourth Amendment explicitly demands." Pet. App. 136a. Further, this Court has never held that the good-faith exception applies when the warrant's defect is that it is an unconstitutional general warrant—as opposed to lacking adequate probable cause. *Cf. Groh v. Ramirez*, 540 U.S.

551, 563-64 (2004) (denying qualified immunity when warrant plainly failed particularization requirement).

The good-faith exception, moreover, should not be extended to this case because it will impede this Court from ever deciding the important constitutional questions presented here.

In the context of a typical search warrant, whether the good faith exception applies or not turns on questions—the amount of information supporting a magistrate's probable cause determination, and the objective reasonability of an officer's reliance on that determination—that vary from case to case. Every geofence warrant, by contrast, is issued based on the same basic set of information: the existence of a crime, a place, and a time, without any particular information as to any particular suspect.

If the good-faith exception applies to geofence warrants based upon that minimum quantum of information, there would be no possible way for a ruling to benefit the person that was searched, regardless of procedural posture. In every civil case, officers will assert qualified immunity based on the current uncertainty in the law. In every criminal case, officers will argue that the very fact that the geofence warrant issued is a sufficient basis to apply the good-faith exception. Indeed, in *Smith*, the Fifth Circuit accepted that very argument. Hence, if the good-faith exception applies, any opinion issued by this Court would be advisory. *See* Kerr, *supra* note 4 (noting, in commentary on decision below, that applying the good-faith exception will result in advisory opinions in every case).

This problem did not arise in *Leon*. In *Leon*, the question was whether evidence should be excluded that was "obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be unsupported by probable cause." 468 U.S. at 900. But questions about probable cause can be resolved in cases not involving warrants, such as vehicle search cases. *See generally Wyoming v. Houghton*, 526 U.S. 295, 300-01 (1999). By contrast, geofence warrant cases always involve warrants based upon the same basic information that vary only in the type of crime and the temporal and geographic scope of the warrant obtained. The disputes turn on whether the warrants are sufficiently particularized and whether a new warrant is needed at the final step before de-anonymizing data. Thus, in *every* case, the government will invoke the good-faith exception merely by virtue of having obtained a warrant, thus preventing any defendant from benefiting from a ruling finding geofence warrants unconstitutional.

That result is untenable. Geofence warrants are a consequential and controversial new type of warrant. This Court should be able to decide whether they are constitutional in a case where its decision actually matters.

This Court's precedents suggest it may relax the good-faith exception under these unusual circumstances. In *Davis v. United States*, 564 U.S. 229 (2011), this Court held that the good-faith exception applies when an officer relies on case law that is subsequently overruled. The defendant raised the concern that no defendant

could ever benefit from a Supreme Court decision overruling precedent, impeding the law's development. In view of that concern, this Court recognized that "in a future case, we could, if necessary, recognize a limited exception to the good-faith exception for a defendant who obtains a judgment overruling one of our Fourth Amendment precedents." *Davis*, 564 U.S. at 248. For similar reasons, the Court should recognize a limited exception to the good-faith exception for a defendant who challenges the legality of a fundamentally new type of warrant issued without any particularized information about any suspect.

CONCLUSION

For the foregoing reasons, this Court should grant the petition.

Respectfully submitted,

GEREMY C. KAMENS
Federal Public Defender
LAURA J. KOENIG
Assistant Federal Public Defender
PATRICK BRYANT
Assistant Federal Public Defender
OFFICE OF THE FEDERAL PUBLIC DEFENDER,
EASTERN DISTRICT OF VIRGINIA
1650 King Street,
Suite 500
Alexandria, VA 22314
(703) 600-0800

ADAM G. UNIKOWSKY
Counsel of Record
LAUREL A. RAYMOND
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
AUnikowsky@jenner.com

APPENDIX

TABLE OF CONTENTS

Appendix A

ON REHEARING EN BANC

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 22-4489

UNITED STATES of America,

Plaintiff – Appellee,

v.

Okello T. CHATRIE,

Defendant – Appellant.

The Reporters Committee for Freedom of the Press; American Civil Liberties Union; American Civil Liberties Union of Virginia; Eight Federal Public Defender Offices Within the Fourth Circuit; Technology Law and Policy Clinic at New York University School of Law; Electronic Frontier Foundation,

Amici Supporting Appellant.

Project for Privacy and Surveillance Accountability, Inc.,

Amicus Supporting Rehearing Petition.

Argued: January 30, 2025

Decided: April 30, 2025

Appeal from the United States District Court for the Eastern District of Virginia, at Richmond. M. Hannah Lauck, District Judge. (3:19–cr–00130–MHL–1)

Before DIAZ, Chief Judge, and WILKINSON, NIEMEYER, KING, GREGORY, AGEE, WYNN, THACKER, HARRIS, RICHARDSON, QUATTLEBAUM, RUSHING, HEYTENS, BENJAMIN, and BERNER, Circuit Judges.

Affirmed by published per curiam opinion in which Chief Judge Diaz, Judge Wilkinson, Judge Niemeyer, Judge King, Judge Agee, Judge Wynn, Judge Thacker, Judge Harris, Judge Richardson, Judge Quattlebaum, Judge Rushing, Judge Heytens, Judge Benjamin, and Judge Berner joined.

Chief Judge Diaz wrote a concurring opinion. Judge Wilkinson wrote a concurring opinion, in which Judge Niemeyer, Judge King, Judge Agee, and Judge Richardson joined. Judge Niemeyer wrote a concurring opinion. Judge King wrote a concurring opinion. Judge Wynn wrote a concurring opinion, in which Judge Thacker, Judge Harris, Judge Benjamin, and Judge Berner joined in full, and in which Judge Gregory joined except as to footnote 1. Judge Richardson wrote a concurring opinion, in which Judge Wilkinson, Judge Niemeyer, Judge King, Judge Agee, Judge Quattlebaum, and Judge Rushing joined. Judge Heytens wrote a concurring opinion, in which Judge Harris and Judge Berner joined. Judge Berner wrote a concurring opinion, in which Judge Gregory, Judge Wynn, Judge Thacker, and Judge Benjamin joined in full, and in which Judge Heytens joined as to Parts I, II(A), and II(B).

Judge Gregory wrote a dissenting opinion.

ARGUED: Michael William Price, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, Washington, D.C., for Appellant. Nathan Paul Judish, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellee. **ON BRIEF:** Geremy C. Kamens, Federal Public Defender, Alexandria, Virginia, Laura J. Koenig, Assistant Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Richmond, Virginia, for Appellant. Kenneth A. Polite, Jr., Assistant Attorney General, Richard W. Downing, Deputy Assistant Attorney General, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C.; Jessica D. Aber, United States Attorney, Kenneth R. Simon, Jr., Assistant United States Attorney, Peter S. Duffey, Assistant United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Richmond, Virginia, for Appellee. Jennifer Lynch, Andrew Crocker, Hannah Zhao, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California; Jacob M. Karr, Technology Law and Policy Clinic, NEW YORK UNIVERSITY SCHOOL OF LAW, New York, New York, for Amici Technology Law and Policy Clinic at New York University School of Law. Jennifer Stisa Granick, San Francisco, California, Nathan Freed Wessler, Ashley Gorski, Patrick Toomey, Brandon Buskey, Trisha Trigilio, Laura Moraff, Brett Max Kaufman, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York; Eden B. Heilman, Matthew W. Callahan, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA, Richmond, Virginia; William F. Nettles, IV, Federal

Public Defender, Columbia, South Carolina, G. Alan Dubois, Federal Public Defender, Raleigh, North Carolina, Louis Allen, Federal Public Defender, Greensboro, North Carolina, Juval O. Scott, Federal Public Defender, Roanoke, Virginia, Brian J. Kornbrath, Federal Public Defender, Clarksburg, West Virginia, John Baker, Federal Public Defender, Charlotte, North Carolina, James Wyda, Federal Public Defender, Baltimore, Maryland, Wesley P. Page, Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Charleston, West Virginia, for Amici American Civil Liberties Union, American Civil Liberties Union of Virginia, and Eight Federal Public Defender Offices Within the Fourth Circuit. Bruce D. Brown, Katie Townsend, Gabe Rottman, Grayson Clary, Emily Hockett, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, Washington, D.C., for Amicus The Reporters Committee for Freedom of the Press. Gene C. Schaerr, Erik S. Jaffe, Aaron C. Ward, SCHAERR | JAFFE LLP, Washington, D.C., for Amicus Project for Privacy & Surveillance Accountability, Inc.

PER CURIAM:

The judgment of the district court is

AFFIRMED.

DIAZ, Chief Judge, concurring:

I join in affirming the district court's denial of Okello Chatrie's suppression motion, but solely on the court's finding of good faith. *See United States v. Chatrie*, 590 F. Supp. 3d 901, 936–41 (E.D. Va. 2022). My colleagues have widely divergent views on the intersection of the Fourth Amendment and the groundbreaking investigative tool at issue here. I respect the care and attention they've devoted to this matter. But judicial modesty sometimes counsels that we not make grand constitutional pronouncements merely because we can.

This is such a case.

I.

A.

Today we consider the constitutionality of geofence warrants, a novel and powerful technology that law enforcement has increasingly used to investigate crime. In simple terms, a geofence warrant requires a service provider to produce location data from cell phone users who were near the scene when a crime occurred.

Like a traditional warrant, law enforcement (as here) may apply for a geofence warrant from a judge. If granted, law enforcement can then serve the warrant on the provider (here, Google).[1]

---

[1] The district court explained: "Other companies such as Amazon and Apple invariably retain users' location data as well. But Google, whose services function across Apple *and* Android devices ..., seems

Google collects the Location History of over 500 million users, and it's this data that law enforcement accesses via a geofence warrant. Location History "appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing location data." *Chatrie*, 590 F. Supp. 3d at 907 (emphasis omitted).

It's also remarkably extensive, "log[ging] a device's location, on average, every two minutes," even "in terms of elevation." *Id.* at 908. If a device is in a building, for example, its Location History can show on which floor.

When presented with a geofence warrant, Google applies an internally developed three-step process, providing to law enforcement an anonymous "list of all Google users whose Location History data indicates were within the geofence during a specified timeframe." *Id.* at 915 (cleaned up). To do this, "Google must search all Location History data to identify users," regardless of whether the users "saved Location History data." *Id.* (cleaned up).[2] After narrowing the list to users who had their Location History enabled, Google also provides "the date and time, the latitude and longitude, the

---

to be subject to more geofence requests than other companies." *Chatrie*, 590 F. Supp. 3d at 907 n.8. What's more, "[c]ompanies such as Apple, Lyft, Snapchat, and Uber have all received geofence warrant requests, but Google is the most common recipient and 'the only one known to respond.'" *United States v. Smith*, 110 F.4th 817, 821 n.2 (5th Cir. 2024) (cleaned up).

[2] Location History "is off by default" on a cell phone, though it's "'possible that a user would have seen the option' to opt into Location History multiple times across multiple apps." *Id.* at 908–09.

geolocation source used, and the map display radius (*i.e.*, the confidence interval)" for the relevant accounts. *United States v. Smith*, 110 F.4th 817, 824–25 (5th Cir. 2025).

At the second step, law enforcement may "compel Google to provide additional location coordinates *beyond* the time and geographic scope of the original request," ostensibly to "assist ... in eliminating devices." *Chatrie*, 590 F. Supp. 3d at 916 (cleaned up). But while law enforcement may widen the geographic scope of the request, Google "typically require[s] law enforcement to narrow the number of users for which it requests [additional] data." *Id.*

Finally, at the third step, law enforcement "'can compel Google to provide *account-identifying information*' for the users 'the [g]overnment determines are relevant to the investigation.'" *Id.* (cleaned up). "This 'account-identifying information' includes the name and email address associated with [an] account." *Id.*

B.

The police charged Chatrie with two crimes related to a bank robbery based on information obtained from Google through a geofence warrant. Detective Joshua Hylton prepared the warrant, which "drew a geofence with a 150-meter radius—with a *diameter* of 300 meters, longer than three football fields—in an urban environment." *Id.* at 918. That radius included the bank and a nearby church. *Id.* The warrant "sought location data for every device present within the geofence" for

an hour around the time of the robbery (i.e., thirty minutes before and thirty minutes after). *Id.* at 919.

In the warrant, Detective Hylton described Google's three-step process, explaining that he would "'attempt to narrow down' the list of users for which the [g]overnment would obtain the most invasive information." *Id.*

First, the warrant directed Google to "'provide "anonymized information" regarding the Accounts that are associated with a device that was inside the described geographical area'" in the hour around the robbery. *Id.* Next, "[l]aw enforcement would return a list of accounts that they had attempted to narrow down," so that "Google would then 'produce contextual data points with points of travel outside of the geographical area." *Id.* (cleaned up). To do so, "the warrant expanded the timeframe to include thirty minutes before and thirty minutes after the initial hour-long window"—covering a two-hour total window. *Id.* Finally, law enforcement would direct Google to provide identifying information for certain accounts.

In his affidavit supporting the warrant, Hylton added that the geofence process could identify not only the robber but also "potential witnesses and/or [other] suspects." *Id.* at 920. This was because the detective had observed on surveillance footage that the robber "had a cell phone in his right hand and appeared to be speaking with someone else on the device"—someone with whom the robber may have been "act[ing] in concert." *Id.* Using the warrant and the subsequent information

Google provided, law enforcement identified Chatrie as a suspect.

After his arrest, Chatrie, who had opted to share his Location History with Google, moved to suppress the location information, arguing that the warrant violated the Fourth Amendment. The district court agreed that *this* geofence warrant "plainly violate[d]" the Constitution,[3] *id.* at 905, but nonetheless declined to suppress it under the good-faith exception to the Fourth Amendment, *id.* at 936–41.

The district court emphasized that "evidence obtained pursuant to a search warrant issued by a neutral magistrate need not be excluded if the officer's reliance on the warrant was 'objectively reasonable.'" *Id.* at 937 (cleaned up). Ticking through the factors the Supreme Court outlined in *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984), that we have since applied, *see, e.g.*, *United States v. Doyle*, 650 F.3d 460, 467 (4th Cir. 2011), the district court found that the instant warrant passed the good-faith bar. *Chatrie*, 590 F. Supp. 3d at 937.

When Detective Hylton applied for the geofence warrant in this case, no court had ruled on the legality of such warrants generally. So he relied on his experience,

---

[3] The Fifth Circuit has held "that geofence warrants are general warrants categorically prohibited by the Fourth Amendment." *Smith*, 110 F.4th at 838. But like the district court here, the Fifth Circuit in *Smith* declined to suppress the challenged warrant on good-faith grounds. *Id.* at 838–40.

having successfully obtained three other geofence warrants after consulting with prosecutors before seeking them. *Id.* at 938.

Hylton also obtained approval from a state magistrate for the warrant. *See id.* at 938–39. To be sure, neither the detective nor the magistrate performed their duties perfectly.

Inexplicably, Detective Hylton submitted a search warrant return—which "notifies the Court when an officer *executes* a search warrant" and describes "what items [the officer] gathered during the search"—to the magistrate before he had even served the warrant on Google. *Id.* at 920. In that return, Hylton "stated that he had executed the warrant," even though, again, he hadn't yet sent it to Google. *Id.* And he wrote that he had seized "Data," when, in fact, he seized "what would be a sizable amount of precise location information on at least nineteen device users." *Id.* (cleaned up).

As for the magistrate, he "asked no questions" of Detective Hylton. Nor did he "seek to modify anything" in the accompanying affidavit, even though this appears to be the first geofence warrant application the magistrate had considered. *Id.* at 918.

Still, the district court was satisfied that the warrant was "not *so* lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* at 937 (cleaned up). The good-faith exception thus saved the warrant from suppression.

I would adopt that narrow holding here.

II.

A.

Geofence warrants are an extraordinary investigatory advancement, born out of technological developments enabling the relentless collection of eerily precise location data. But questions remain about the technology enabling such warrants as well as Google's process for responding to them. It's no mystery then that applying our legal precedents to this rapidly evolving technology is precarious. Indeed, as the district court noted, "[t]his case implicates the next phase in the courts' ongoing efforts to apply the tenets underlying the Fourth Amendment to previously unimaginable investigatory methods." *Chatrie*, 590 F. Supp. 3d at 905.

Earlier cases applied the Fourth Amendment to "recording devices in public telephone booths," "thermal-imaging equipment" aimed at homes, "and, most recently, to cell-site location data." *Id.* (summarizing cases). The cases have protected "data that provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations,'" if that data hasn't been meaningfully disclosed to a third party. *Carpenter v. United States*, 585 U.S. 296, 311, 314–15, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018).[4]

---

[4] The Court opined that whether and how the Fourth Amendment applied to cell-site records existed "at the intersection of two lines of cases, both of which inform[ed] [its] understanding of the privacy interests at stake." 585 U.S. at 306, 138 S.Ct. 2206. "The first set of

We've then used this precedent to "solidif[y] the line between short-term tracking of public movements—akin to what law enforcement could do prior to the digital age—and prolonged tracking that can reveal intimate details through habits and patterns." *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (en banc) (cleaned up). The latter "invades the reasonable expectation of privacy that individuals have in the whole of their movements and therefore requires a warrant." *Id.*

Still, the Supreme Court has recognized that our existing Fourth Amendment frameworks—like the third-party doctrine—may be "ill suited to the digital age," *United States v. Jones*, 565 U.S. 400, 417–18, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (Sotomayor, J., concurring), particularly when applied to cell phones, which can enable law enforcement to "achieve[ ] near perfect surveillance," *Carpenter*, 585 U.S. at 312, 138 S.Ct. 2206.[5] On top of that, cell phones have become

---

cases"—including *United States v. Knotts*, 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), and *United States v. Jones*, 565 U.S. 400, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012)—"address[ed] a person's expectation of privacy in his physical location and movements." *Carpenter*, 585 U.S. at 306–07, 138 S.Ct. 2206. "In a second set of decisions"—including *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)—"the Court [drew] a line between what a person keeps to himself and what he shares with others," which is the guiding principle for the third-party doctrine. *Carpenter*, 585 U.S. at 307–09, 138 S.Ct. 2206.

[5] Even Google—in an amicus brief—argued "that a geofence is certainly a "'search" within the meaning of the Fourth Amendment' because 'users have a reasonable expectation of privacy in the [Location History] information, which the government can use to

"almost 'a feature of human anatomy'" that individuals "compulsively carry ... with them all the time." *Id.* at 311, 138 S.Ct. 2206 (cleaned up).

So what happens when (as here) there are serious questions about the scope of a defendant's consent to a third-party's use of his data given the breadth of the third party's "detailed, encyclopedic, and effortlessly compiled" data collection methods? *Id.* at 309, 138 S.Ct. 2206; *see also id.* at 315, 138 S.Ct. 2206 (commenting that exposure of data may not be meaningfully voluntary when the user doesn't "'assume the risk' of turning over a comprehensive dossier of his physical movements" (cleaned up)). Or when (again as here) a "brief snapshot" of location information, even if it doesn't capture a pattern, still "expose[s] highly sensitive information—think a visit to 'the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club ..., [or] the mosque, synagogue[,] or church'"? *Smith*, 110 F.4th at 833 (cleaned up); *see also Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206 ("A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.").

Despite the district court's best efforts to develop the record, our understanding of Google's data collection policy and its internal geofence warrant process remains imperfect and incomplete.[6] It's no surprise then that the

---

retrospectively reconstruct a person's movements in granular detail.'" *Chatrie*, 590 F. Supp. 3d at 907 n.5 (cleaned up).

[6] To add more uncertainty, Google intends to change its Location History policy so that it will no longer be able to respond to geofence

parties vigorously debate—as my colleagues do—the potentially sweeping implications of any decision.

One camp insists that disallowing geofence warrants would contravene our precedent, hamstring law enforcement in investigating crimes, and chill innovation at any private company that handles a large database of users. The other camp is just as adamant that granting blanket approval to these warrants would contravene our precedent and compromise the privacy interests of cell phone users.

The balance, ever so delicate, swings from law enforcement and public safety to liberty and privacy interests depending on the record facts. Yet despite a shallow well of information and legal authority and a litany of unanswered questions as to our decision's reach, my colleagues choose to write broadly. At least in this case, I would opt for restraint and rest on the good-faith exception to the Fourth Amendment.[7]

---

warrants. *See Smith*, 110 F.4th at 822 n.3.; *see also* Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, Google (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps/ [https://perma.cc/7ZMS-RHF9].

[7] *See, e.g.*, *Ashwander v. Tenn. Valley Auth.*, 297 U.S. 288, 347, 56 S.Ct. 466, 80 L.Ed. 688 (1936) (Brandeis, J., concurring) ("The Court will not pass upon a constitutional question although properly presented by the record, if there is also present some other grounds upon which the case may be disposed of."); *Camreta v. Greene*, 563 U.S. 692, 707, 131 S.Ct. 2020, 179 L.Ed.2d 1118 (2011) ("In general, courts should think hard, and then think hard again, before turning small cases into large ones.").

B.

The good-faith exception is reason enough to affirm the district court without stunting our ability to respond down the line to Fourth Amendment issues that are presently "unimaginable." *Chatrie*, 590 F. Supp. 3d at 905. Arising out of the exclusionary rule, the exception broadly queries the deterrent benefits of suppressing an otherwise constitutionally infirm search. *See, e.g., Davis v. United States*, 564 U.S. 229, 236–37, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011).

Generally, "[t]o 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." *Herring v. United States*, 555 U.S. 135, 144, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009). And "'[u]sually, 'a warrant issued by a magistrate ... suffices to establish'" that a law enforcement officer has "acted in good faith in conducting the search." *Doyle*, 650 F.3d at 467 (quoting *Leon*, 468 U.S. at 922, 104 S.Ct. 3405).

To better measure any deterrent benefits, courts consider four circumstances in which good faith won't shield even a search made pursuant to a warrant:

> (1) If the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) if the issuing magistrate wholly abandoned his judicial role ... ; (3) if the affidavit supporting the warrant is so lacking in indicia of

> probable cause as to render official belief in its existence entirely unreasonable; and (4) if under the circumstances of the case the warrant is so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.

Id. at 467 (cleaned up). None defeat good faith here.

As to the first, Hylton's occasional sloppiness aside, there's no evidence that Hylton gave false information to the magistrate when seeking the geofence warrant. And I agree with the government that Chatrie expressly disclaimed any challenge under *Franks v. Delaware*, 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978), that Detective Hylton "intentionally or recklessly omitted material information from the affidavit." *See* Appellee's Br. at 50 (quoting *United States v. Pulley*, 987 F.3d 370, 376 (4th Cir. 2021)); *see also* Appellant's Br. at 11 n.2.

Nor is there evidence that the magistrate didn't review the warrant application and Hylton's affidavit before issuing the warrant, or that the magistrate at any time "overstepped his ... judicial responsibilities and compromised his judicial neutrality." *Chatrie*, 590 F. Supp. 3d at 938 (cleaned up). Chatrie's citation to *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 99 S.Ct. 2319, 60 L.Ed.2d 920 (1979), in which the magistrate became "a member, if not the leader, of the search party which was essentially a police operation," *id.* at 327, 99 S.Ct. 2319, is a far cry from the magistrate's performance here.

At best, Chatrie has "perhaps[ ] shown that [the magistrate] *should have* considered the implications of

the [w]arrant more carefully." *Chatrie*, 590 F. Supp. 3d at 938. But our standard for good faith is not so exacting. The magistrate remained a neutral authority who reviewed a warrant application describing a novel investigative tool with a "dearth of court precedent to follow." *Smith*, 110 F.4th at 840.[8]

Chatrie's fight isn't really with the police or the magistrate. Rather than allege any malfeasance by either, Chatrie repackages his attack on the warrant's probable cause and particularity to suggest that both acted in bad faith. *See*, *e.g.*, Appellant's Br. at 29–30, 32–33, 38–39. He argues that the warrant was "'completely devoid' of probable cause," *id.* at 23, and so "profoundly lacking in particularity," *id.* at 34, as to render it a "despised" (and illegal) general warrant, *id.* at 35.

A few points bear repeating. Hylton reviewed surveillance footage showing that the robber used a cell phone, so he knew that a geofence could reveal both the robber's identity and any potential co-conspirators. The detective also limited the warrant geographically and temporally. Hylton, of course, could have further limited the warrant to a smaller radius around the Bank or a closer time to the robbery. But given the "dearth of ... precedent to follow," *Smith*, 110 F.4th at 840, nothing required or cautioned him to do so.

---

[8] Despite holding that geofence warrants are categorically unconstitutional general warrants, our sister circuit declined to suppress the evidence under the good-faith exception. *Smith*, 110 F.4th at 840.

Without any directly governing case law, Hylton understandably relied on the previous guidance he had been given, which is, as my colleague explains, "what we expect reasonable officers to do when faced with such uncertainty." Opinion of HEYTENS, J., at 87 (concurring). Magistrates and prosecutors had approved three of Hylton's "mostly similar" prior warrants—"all but one [of which] incorporated a roughly 150-meter radius." *Chatrie*, 590 F. Supp. 3d at 938. As the district court found, "[e]ven accounting for his miscues, in light of the complexities of this case, Det[ective] Hylton's prior acquisition of three similar warrants, and his consultation with [g]overnment attorneys before obtaining those warrants, the [c]ourt cannot say that [his] reliance on the instant warrant was *objectively unreasonable*." *Id.* (emphasis added).

Chatrie insists that even a warrant "cloaked" in new technology must still be supported by probable cause and be sufficiently particularized as to the places to be searched and things to be seized. Appellant's Br. at 24. I agree with him. But Detective Hylton limited the places to be searched—both by geography and time—as well as the location information to be seized—to those cell phone users within the parameters of the geofence warrant.

To the extent that Chatrie complains that law enforcement didn't know his identity in seeking the warrant (or until well into Google's three-step process), I'm not persuaded that carries the day, especially when assessing good faith. For many warrants, after all, the point is to identify a suspect, which is why the warrant requirement focuses on the *places* to be searched and *things* to be seized. *See Zurcher v. Stanford Daily*, 436

U.S. 547, 555, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978) ("Search warrants are not directed at persons; they authorize the search of 'places' and the seizure of 'things,' and as a constitutional matter they need not even name the person from whom the things will be seized." (cleaned up)).

Take *Zurcher v. Stanford Daily*, 436 U.S. 547, 98 S.Ct. 1970, 56 L.Ed.2d 525, in which law enforcement executed a search warrant of the student newspaper's offices to seize "negatives, film, and pictures showing the events and occurrences at the [Stanford University Hospital] on the evening" that demonstrators allegedly assaulted police officers. *Id.* at 551, 98 S.Ct. 1970. Law enforcement secured the warrant "on a finding of 'just, probable and reasonable cause for believing that'" the things seized—negatives, photographs, and films—would reveal "evidence material and relevant to the identity of the perpetrators." *Id.* And the warrant was issued even though the affidavit "contained no allegation or indication that members of the Daily staff were in any way involved in unlawful acts at the hospital." *Id.*

No doubt, the initial search here of over 500 million cell phone users is—to put it mildly—broader than the search of a handful of college students, but both warrants were issued to help identify the suspect of the crime. And in this case, law enforcement narrowed down the list of potential perpetrators at each step of the process from millions to dozens to a few based on the other relevant evidence. That rings in probable cause sufficient for me to find good faith.

Geofence warrants may differ from traditional warrants, working in reverse by specifying the time and place of a crime rather than the identity of the perpetrator, but that doesn't automatically render them "facially deficient," *Doyle*, 650 F.3d at 467 (cleaned up). Indeed, most Internet or mass database searches would be cut from the same cloth.

All this is to say that it's not clear what conduct suppression of the evidence would "meaningfully deter" here. *Herring*, 555 U.S. at 144, 129 S.Ct. 695; *accord Chatrie*, 590 F. Supp. 3d at 938. Whatever the warrant's shortcomings, I agree with the district court that the warrant wasn't "*so* lacking in indicia of probable cause" as to justify suppressing it here. *Chatrie*, 590 F. Supp. 3d at 937 (cleaned up).

III.

When confronted with another opaque and "transformative" piece of technology, the Supreme Court recently reminded us that

> [t]his challenging new context counsels caution on our part. As Justice Frankfurter advised 80 years ago in considering the application of established legal rules to the "totally new problems" raised by the airplane and radio, we should take care not to "embarrass the future."

TikTok Inc. v. Garland, —— U.S. ——, 145 S. Ct. 57, 62, 220 L.Ed.2d 319 (2025) (per curiam) (cleaned up).

My colleagues have done their level best to cut through the Fourth Amendment fog in this case. In contrast,

some may say that I've done nothing more today than kick the geofence warrant can down the road. Others may complain that I've offered no guidance to law enforcement and magistrates about the reach of the Fourth Amendment in the digital age, or worse still, that I've resorted to "judicial abdication," opinion of WYNN, J., at 35 (concurring).

But what guidance have my colleagues given today? Instead of a Fourth Amendment compass, we've gifted law enforcement (and the public) a labyrinth of—by my count, nine—advisory opinions, many pointing in different directions.[9] *See, e.g.*, *Riley v. California*, 573 U.S. 373, 398, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014) (expressing a "preference" for "provid[ing] clear guidance to law enforcement" under the Fourth Amendment); Felix Frankfurter, *A Note on Advisory Opinions*, 37 Harv. L. Rev. 1002, 1008 (1942) ("It must be remembered that advisory opinions are not merely advisory opinions. They are ghosts that slay."). I don't see the utility in that, as it assumes (wrongly) that we must give a full answer now.

In short, there are times to make sweeping constitutional pronouncements (with attendant

---

[9] Even the Fifth Circuit's opinion, though issued in one voice, has left legal scholars concerned about its fidelity to the Supreme Court's Fourth Amendment precedent, and its implications for all manner of law enforcement investigative tools. *See, e.g.*, Orin S. Kerr, *The Fifth Circuit Shuts Down Geofence Warrants—And Maybe a Lot More*, The Volokh Conspiracy (August 13, 2024), https://reason.com/volokh/2024/08/13/fifth-circuit-shuts-down-geofence-warrants-and-maybe-a-lot-more/ [https://perma.cc/3G5V-WE7F].

consequences) and times to wait. Humility in the face of the unknown—whether it be the legal ramifications or practical consequences of our decision, or Google's own changing policies—"counsels caution." *TikTok, Inc.*, 145 S. Ct. at 62.

* * *

A brief coda. I expect law enforcement to exercise good faith in using powerful, revolutionary technologies to investigate crimes, and, indeed, that their first instinct will be to use and not abuse the information this technology reveals. And I echo the district court's warning that "[d]espite ... finding good faith here, ... this exception may not carry the day in the future." *Chatrie*, 590 F. Supp. 3d at 941.

By my measure, today "our judicial obligation" can "be captured by a much older rule, familiar to every doctor of medicine: 'First, do no harm.'" *Denver Area Educ. Telecomms. Consortium, Inc. v. F.C.C.*, 518 U.S. 727, 778, 116 S.Ct. 2374, 135 L.Ed.2d 888 (1996) (Souter, J., concurring).

WILKINSON, Circuit Judge, with whom NIEMEYER, KING, AGEE, and RICHARDSON, Circuit Judges, join, concurring:

With due regard for my fine colleagues, there was no search here. And even if one were to assume there was a search, there are many good reasons why courts should respectfully reject the assault on geofence warrants mounted by appellant, several of my colleagues, *see* opinion of WYNN, J. (concurring), and the Fifth Circuit Court of Appeals, *see United States v. Smith*, 110 F.4th 817 (5th Cir. 2024).

I.

There was no search because this case involved a straightforward application of *Smith*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), and *Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). Just like in those cases, Chatrie volunteered incriminating information about himself to a third party. His expectation of privacy was comparatively small. *Miller*, for instance, involved months of financial transaction history, which undeniably exposes many intimacies of one's life. If that request for bank records was permissible, surely this request for a two-hour snapshot of one's public movements, which hardly reveals one's habits, is okay.

There are many good reasons why the Supreme Court did not discard the third-party doctrine for all location data requests. Of course the concern for privacy in all of its dimensions was central to the Framers' contemplation. But the Fourth Amendment, to state the obvious, calls also for a balance between individual

privacy and public safety. Favoring one over the other is at odds with the textual "touchstone" of the Amendment, which is reasonableness. *See Maryland v. King*, 569 U.S. 435, 448, 133 S.Ct. 1958, 186 L.Ed.2d 1 (2013). Respecting Fourth Amendment balance means protecting "that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter v. United States*, 585 U.S. 296, 305, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018). Not less, of course. But also not more.

So yes, the Bill of Rights stands vigilant guard against the abuses of the state. The Fourth Amendment is itself a prime illustration of its function. Yet privacy is also threatened by, say, a theft of personal items. And privacy is in part a peace of mind. The prospect of criminal malefactors intruding on that peace can only mean our privacy has been compromised. That the transgression is attributable to private actors does not mean it cannot be part of the calculus of reasonableness which, again, is our Fourth Amendment touchstone. Seen in this light, privacy is not invariably in an adversarial relationship with the state, but something the state can take measured steps to protect and provide.

II.

Even if there was a search, there is no room for emergent judicial hostility toward this new investigative tool. Disabling the government from using geofence location data would spurn the basic Fourth Amendment balance and undermine legitimate law enforcement in at least three basic ways.

One, this restraint on investigative tools would frustrate law enforcement's ability to keep pace with tech-savvy criminals. Lawless actors of all kinds are growing more sophisticated and leveraging new technologies to commit crimes and evade detection. Transnational criminal organizations rely on digital currencies and encrypted communications to conceal their violence and fraud. 2023 WHITE HOUSE STRATEGY TO COMBAT TRANSNATIONAL ORGANIZED CRIME 3–4, 21 (2023). Terrorists likewise deploy emerging technologies like encryption, biotechnology, and artificial intelligence. Ian Moss, U.S. Dep't of State, *Opening Remarks on Addressing Emerging Technology in the Realm of Racially or Ethnically Motivated Violent Extremism* (Feb. 14, 2024). Even small-time pimps encrypt their devices to block lawful access to their databases of sex-trafficking victims. *See Lawful Access*, Office of Legal Policy, U.S. Dep't of Justice (Nov. 18, 2022). Examples abound. In this age of innovation, those who would break the law spare no expense to employ the latest and greatest technological tools.

All the while, under appellant's view, local, state, and federal officers would lose the tools they need to protect the public from the modern-day criminal. More cold cases would go unsolved. Think of a murder where the culprit leaves behind his encrypted phone and nothing else. No fingerprints, no witnesses, no murder weapon. But because the killer allowed Google to track his location, a geofence warrant can crack the case. *See* Damien Christopher & Nick Penzenstadler, *Cold Cases Cracked by Cellphones: How Police Are Using Geofence Warrants to Solve Crimes*, USA TODAY (Sept. 8, 2022).

Taking this tool of last resort out of law enforcement's hands would leave these case files collecting dust. The Fourth Amendment does not require allowing criminals to take advantage of cutting-edge technologies while preventing the government from doing the same. Technology enables the lawbreaker. Courts disable the government. This imbalance will only grow with time.

Two, law enforcement under appellant's view would be robbed of valuable channels of communication with the private sector. This case is a good example of those channels at work. Chatrie, like one-third of Google users, signed up for a program that shared his location data with Google. In return he got a "virtual journal of his past travels" and "real-time traffic updates." *United States v. Chatrie*, 107 F.4th 319, 322 (4th Cir. 2024), *panel opinion vacated by order of the en banc court* (Nov. 1, 2024). And because he brought his phone to the robbery, the government was able to place Chatrie at the crime scene with Google's help.

Chatrie would shut down this kind of sensible public-private cooperation. Doing so would override the equilibrium between user privacy and public safety that has emerged organically, without judicial intervention, from an ecosystem of customers, companies, and law enforcement. Critics seem to presuppose that private companies such as Google are naturally disposed to compromise the privacy of their users. Quite the contrary. Google has every incentive to protect the privacy of those who utilize its services. Not to do so risks damaging its business.

The procedures used by Google here prove the point. In responding to the government's location data request, Google insisted on a rigorous "three-step process" to protect user privacy. *Chatrie*, 107 F.4th at 324. It kept all data anonymized until officers were able to zero in on a small group of suspects. Only then did Google disclose the identities of Chatrie and two others. Far from a "digital dragnet," the process used here reflected the reasonable balance between privacy and safety that the Fourth Amendment envisioned. By urging us to rule broadly that geofence warrants are impermissible, Chatrie would unleash a fear of legal liability that would chill data sharing between public and private sectors and foreclose fruitful communication over the respective values of personal privacy and effective law enforcement.

Three, some of my colleagues go down a dangerous road by casting the use of geofence data as some new monster. True, the technology is new, but the technique is a familiar one. In fact the technique is not too different from the traditional winnowing methods that criminal investigators have always used. Investigations often start out broad. Culprits are not always known, crime scenes may be crowded, and detectives have to start somewhere. They canvass the surroundings, review security footage, and pick out and rule out persons of interest. Analysis of geofence data follows this same narrowing progression. So too do keyword searches and tower dumps. Will courts put a stop to those too? *See* Orin Kerr, *The Fifth Circuit Shuts Down Geofence Warrants—And Maybe a Lot More*, LAWFARE (Aug. 14, 2024). Will courts seek to disable law enforcement in cases where there are no eyewitnesses and few forensic

clues? If so, they are far ahead of the Supreme Court in *Carpenter*, which ruled on seven days' worth of location data, not the snapshot before us now.

III.

There is a further difficulty with categorically invalidating geofence warrants, namely that of extending the exclusionary rule with no regard to its costs. In *Hudson v. Michigan*, 547 U.S. 586, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006), the Supreme Court cautioned against the rule's "indiscriminate application" and reiterated that it should apply only when the "deterrence benefits" outweigh the "social costs." *Id.* at 591, 126 S.Ct. 2159. The social costs here are significant. As we have explained, geofence location data is often the only way to identify and convict perpetrators like Chatrie. Excluding this evidence from trial gives these criminals, in the words of the Supreme Court, "a get-out-of-jail-free card." *Id.* at 595, 126 S.Ct. 2159. A reflexive expansion of the exclusionary rule ignores the primary allegiance of courts to probative evidence and neglects the Supreme Court's clear instructions in *Hudson*.

The creation of remedies involves the weighing of costs and benefits, which often falls within the domain of legislators. Indeed, legislatures routinely enact laws balancing the competing considerations of personal privacy and public safety. For instance, the Electronic Communications Privacy Act, Pub. L. No. 99–508, 100 Stat. 1848 (1986), authorizes the government to collect people's communications and digital data for law enforcement purposes. But the law offers a *range* of procedural safeguards—anything from an

administrative subpoena to a court-issued warrant based on probable cause—and remedies depending on the nature of the data. This type of compromise is a classic legislative task. Applying the exclusionary rule categorically to geofence warrants preempts legislative input in an area whose real impact upon the body politic would seem to invite some measure of popular participation.

IV.

As we contemplate the future, Fourth Amendment interpretation leads to twin risks. One is the risk that privacy will succumb to the evermore invasive technological capabilities at the hands of an evermore intrusive state. The other risk, which is just as real, is that of privileging those who break the law over those who would enforce it. Either future portends stark consequences for society where individual dignity cannot in the end be divorced from an intuitive sense of personal safety.

The facts of this case are illustrative. Chatrie terrorized the employees and patrons of the Call Federal Credit Union in Midlothian, Virginia. He walked into the bank armed with a handgun, told the teller that he had accomplices outside and that he was holding her family hostage, and threatened to "hurt[ ] everyone in sight" if she called the cops. *United States v. Chatrie*, 590 F. Supp. 3d 901, 905–06 (E.D. Va. 2022). Brandishing his gun, he forced everyone to the ground and ordered the manager to empty the safe. Chatrie was able to escape with $195,000. Because he was not apprehended at the scene, he eluded law enforcement for months. Officers

were out of traditional leads. Only the geofence warrant eventually allowed police to track Chatrie down and restore a sense of resolution to the community. Without geofence location data, crimes even more serious than this one will escape detection.

The sheer breadth of appellant's position is disquieting. Those who support it seek a broad judicial declaration that geofence warrants would be unconstitutional in all their forms, no matter how specific and particularized. The geofence warrant here was closely confined to a particular time, place, and incident. There can be abuses to be sure, but courts can review the temporal and spatial character of these warrants as we would any Fourth Amendment claim. To strike the warrant down here comes pretty nearly to invalidating it everywhere. No matter says appellant. All such warrants are on the chopping block.

Crime invades privacy. Crime limits freedom and narrows space. The fact that the Fourth Amendment exists to check the undeniable excesses of the modern state does nothing to diminish the fact that crime imperils the very values the Fourth Amendment exists to protect. The Framers resolved this dilemma by making reasonableness the Amendment's touchstone. It is dispiriting that some would proceed with nary a thought given to that two-sided balance which reasonableness above all denotes. It will never do to see the future with but a single eye.

NIEMEYER, Circuit Judge, concurring:

I am pleased to join the opinions of Judge Wilkinson and Judge Richardson in full. Today's Fourth Amendment caselaw often starts with a pre-Internet analogy. *See Carpenter v. United States*, 585 U.S. 296, 306, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018). I write separately because I believe that a commonsense analogy dictates the same result reached by the opinions of Judge Wilkinson and Judge Richardson.

To begin, the Fourth Amendment protects the people "in their persons, houses, papers, and effects" against unreasonable searches. U.S. Const. amend. IV. It has also been construed to extend beyond those textual objects to protect certain expectations of privacy. *See Katz v. United States*, 389 U.S. 347, 353, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); *id.* at 361, 88 S.Ct. 507 (Harlan, J., concurring). And recently, the Supreme Court held in *Carpenter* that the Fourth Amendment protects a person's expectation of privacy in "the whole of his physical movements." 585 U.S. at 313, 138 S.Ct. 2206. Thus, when law enforcement, without a warrant, accesses a person's continuously collected and automatically generated cell-site location information, it violates that expectation of privacy. *See id.* at 315–16, 138 S.Ct. 2206. But *Carpenter* left in place many existing limits on the scope of the Fourth Amendment. Apart from protecting the unique data-collection system at issue there, the *Carpenter* Court explained that it was not "disturb[ing] the application" of the third-party doctrine "or call[ing] into question conventional surveillance techniques and tools, such as security cameras. Nor [did it] address other business records that

might incidentally reveal location information." *Id.* at 316, 138 S.Ct. 2206.

One of the "conventional surveillance techniques" that *Carpenter* left untouched is law enforcement's practice of collecting and following "markers," or clues, voluntarily left behind and abandoned by a person at the scene of a crime or in connection with the crime. These markers can reveal who committed the crime, and, when the crime was committed in a public place or in the place of a third person, they may be collected by law enforcement without a warrant. Thus, law enforcement is entitled to retrieve boot prints, tire tracks, shell casings, a scarf or a cap, and items left with fingerprints or DNA on them. Similarly, they can retrieve third-person records of a suspect's presence, such as pictures and videos taken routinely at the scene, records of tolls paid, or records of credit card transactions. Indeed, such third-party records might include a note left with a teller during a bank robbery. Collecting markers such as these from public places or third persons is the stuff of law enforcement, enabling it to solve crimes and prosecute suspects, and the person who left them behind is not "searched" in his person and effects, in violation of the Fourth Amendment.

Of course, if a person were careful not to leave footprints, fingerprints, shell casings, or other markers behind, law enforcement would have to turn to other techniques and strategies to advance its investigation. But when such markers are left behind, law enforcement should not be denied the benefit of the person's carelessness when solving a crime. And *Carpenter* says nothing to the contrary. What *Carpenter* does say is that

law enforcement needs to obtain a warrant before it utilizes digital technology to track a citizen's long-term movements — "the whole of his physical movements" — at least when that person is, in effect, compelled to leave behind a digital footprint wherever he goes. 585 U.S. at 313, 315, 138 S.Ct. 2206; *see also United States v. Jones*, 565 U.S. 400, 430, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (Alito, J., concurring in the judgment); *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (en banc). But those features are not present here, and, as this case is otherwise well-removed from the text of the Fourth Amendment, I would hold that law enforcement did not conduct a search.

This case relates to law enforcement's effort to collect markers from third persons voluntarily left behind by a person during the commission of a crime. In this case, the person left behind electronic location data that he voluntarily transmitted from the scene of the crime by his cell phone. Law enforcement did not collect the data from the person or the person's cell phone, which would require a warrant, *see Riley v. California*, 573 U.S. 373, 401, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014), but from a third person who received the person's voluntarily transmitted data and stored them in a data bank, *see Smith v. Maryland*, 442 U.S. 735, 743–44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); *United States v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). In this sense, the data, when limited to the time and place of the crime, were no different than any other marker left behind by a perpetrator.

What might distinguish such electronic data from other markers is the scope of the data collection. Here, the

data were retained by the third person in a large data bank — Google's Sensorvault — which includes information unrelated to the time and place of the crime. The broad scope of that data bank could raise privacy concerns for those whose data were stored there, including the suspect's data that did not constitute a marker from the crime scene. But law enforcement accessed only two hours' worth of location data, which is far from "the whole of [anyone's] physical movements." *Carpenter*, 585 U.S. at 313, 138 S.Ct. 2206. And law enforcement relied on procedures designed to isolate the data constituting markers left behind at the crime scene from other, unrelated data, which helped mitigate any privacy concerns.

The geofence warrant issued in this case initially required Google to produce data transmitted by cell phones only (1) from the scene of the crime and (2) during the time when the crime was committed. They were thus potential crime markers, which helped law enforcement solve the crime and were not materially distinct from the fingerprints or shell casings left behind by a prior era's less-than-careful perpetrators.

At bottom, this case is a good example of law enforcement properly balancing its need to solve and prosecute crimes with citizens' privacy concerns under the Fourth Amendment. Neither the suspect nor any other person whose data was stored in the data bank could legitimately claim, in view of the procedures followed, that his rights were violated. Judge Richardson's opinion neatly, systematically, and accurately sets forth the legal principles supporting this conclusion, and Judge Wilkinson's opinion elegantly

articulates the public policies that this conclusion promotes.

In addition, I also concur in the judgment of the court holding that, in any event, law enforcement's collection of the data from Google was protected because law enforcement relied in good faith on a warrant issued by a detached and neutral judicial officer. *See United States v. Leon*, 468 U.S. 897, 922–23, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).

KING, Circuit Judge, concurring:

I am pleased to join in the fine concurring opinions of Judge Wilkinson and Judge Richardson. In addition, I agree that the officers acted in good faith, and I therefore also support the affirmance of the district court's judgment on that basis.

WYNN, Circuit Judge, with whom Judges THACKER, HARRIS, BENJAMIN, and BERNER join, and with whom Judge GREGORY joins except as to footnote 1, concurring in the judgment:

The surveillance technologies at issue in this case—the very same ones that seem to thrill my colleagues who join Judge Wilkinson's separate opinion—would have been unimaginable to the Founders. Yet, in *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018), our Supreme Court rightly recognized that the principles enshrined in the Fourth Amendment do not wither in the face of advancing technologies. Rather, they must be vigorously protected from ever-expanding methods of government intrusion.

The Court in *Carpenter* reaffirmed a fundamental truth: until, and unless, the Constitution is amended, it is the duty of the judiciary to defend constitutional rights against encroachments that the Framers could not have foreseen but surely would have found intolerable.

Thus, "when a Fourth Amendment case presents a novel question of law whose resolution is necessary to guide future action by law enforcement officers and magistrates, there is sufficient reason for [a court] to decide the violation issue before turning to the good-faith question." *United States v. Bosyk*, 933 F.3d 319, 332 n.10 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 264, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983) (White, J., concurring)); *see United States v. Leon*, 468 U.S. 897, 925, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). "As demonstrated by the divergent decisions of district courts"—and here,

of circuit courts—"this is one such case." *Bosyk*, 933 F.3d at 332 n.10.

The constitutional question in this case has been fully briefed, argued and exhaustively debated—not only by the parties but by amici and members of this Court. And it is unclear what future case could better tee up the issue. Judicial modesty does not demand judicial abdication.

Yet, by declining to reach the merits in this matter, this Court squanders a critical opportunity to clarify the Fourth Amendment's application to emerging surveillance technologies. Instead, we take shelter in the judge-made doctrine of "good faith," leaving both courts and citizens to grope in the dark as to the limits of governmental power in the digital age. The result? Individuals subject to sweeping, sophisticated surveillance with little or no judicial oversight—an outcome wholly at odds with our constitutional design.

I therefore write separately to explain why, in obtaining Google Location History data traceable to Okello Chatrie, the police conducted a Fourth Amendment search.[1]

I.

The Fourth Amendment promises "secur[ity] ... against unreasonable searches and seizures." U.S. Const.

---

[1] Although I believe that this case involved a Fourth Amendment search—and that we should say so—I acknowledge that the conditions for application of the good-faith exception to the exclusionary rule are met here.

amend. IV. Surveillance technologies, though also deployed in the name of security, pose a dynamic and resilient threat to that right. Technology continually advances; consequently, maintaining the balance between individual privacy and public safety requires vigilance. Recognizing this, the Supreme Court has allowed Fourth Amendment jurisprudence to evolve alongside technology. I begin by surveying that evolution, with particular attention to its latest chapter: the Court's decision in *Carpenter*.

A.

Early Supreme Court decisions made clear that a government agent's physical trespass into a private space is a search, and thus requires a warrant. But as the Government's capacity to surveil at a distance expanded, so did the Fourth Amendment's protections. *See Carpenter*, 585 U.S. at 304, 138 S.Ct. 2206. The modern rule—adapted from Justice Harlan's concurring opinion in *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), and reaffirmed many times since—is that "[w]hen an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable, ... official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Carpenter*, 585 U.S. at 304, 138 S.Ct. 2206 (internal quotation marks omitted).

In the 1970s and 1980s—before the internet age—the Supreme Court placed two key limitations on *Katz*'s expansion of recognized Fourth Amendment protections: the third-party and public-surveillance

doctrines. *See id.* at 306–09, 138 S.Ct. 2206. Understanding those limitations is essential to understanding the Court's later decision in *Carpenter*.

First, the third-party doctrine stems from decisions issued over 45 years ago: *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), and *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976).

In *Smith*, police used a pen-register device to collect phone numbers the suspect dialed on his home phone. *Smith*, 442 U.S. at 737, 99 S.Ct. 2577. And in *Miller*, police accessed the suspect's bank records, such as checks and deposit slips. *Miller*, 425 U.S. at 437–38, 96 S.Ct. 1619. The Supreme Court held that the suspects had no reasonable expectation of privacy in those relatively unrevealing records, which the suspects had voluntarily exposed to third parties in the ordinary course of business. *See Smith*, 442 U.S. at 737, 741–42, 99 S.Ct. 2577; *Miller*, 425 U.S. at 440–43, 96 S.Ct. 1619; *Carpenter*, 585 U.S. at 308–09, 138 S.Ct. 2206 (discussing *Smith* and *Miller*).

Second, the public-surveillance doctrine emerges from decisions issued over 40 years ago, and centers on differing expectations of privacy in *public* versus *private* spaces.

In *United States v. Knotts*, 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), the Court held that police did *not* conduct a Fourth Amendment search when they used a "beeper"—that is, "a radio transmitter" that "emits periodic signals that can be picked up by a radio

receiver"—to keep a vehicle in view during a single drive "on public thoroughfares." *Id.* at 277, 281, 103 S.Ct. 1081. The Court reasoned that police could have tracked the vehicle's movements without the beeper—by physically following it—so the suspect had no reasonable expectation of privacy in those movements. *Id.* at 281–82, 285, 103 S.Ct. 1081.

Knotts "was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance." *Carpenter*, 585 U.S. at 306, 138 S.Ct. 2206. The Court stressed that the beeper merely "augment[ed]" the officers' own "sensory faculties." *Knotts*, 460 U.S. at 282, 103 S.Ct. 1081. And it cautioned that, should "twenty-four hour surveillance of any citizen" become "possible," "different constitutional principles may be applicable." *Carpenter*, 585 U.S. at 306–07, 138 S.Ct. 2206 (quoting *Knotts*, 460 U.S. at 283–84, 103 S.Ct. 1081).

The Court distinguished *Knotts* in *United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984), which held that police conducted a Fourth Amendment search when they used a beeper to track a container as it moved between commercial lockers and private residences. *Id.* at 708–10, 714–18, 104 S.Ct. 3296. The Court explained that because "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable," "[s]earches and seizures inside a home without a warrant are presumptively unreasonable absent exigent circumstances." *Id.* at 714–15, 104 S.Ct. 3296. Although

tracking the beeper's location was "less intrusive than a full-scale search," it "reveal[ed] a critical fact about the interior of the premises"; and unlike the public movements of the vehicle in *Knotts*, police "could not have otherwise obtained [that information] without a warrant." *Id.* at 715, 104 S.Ct. 3296.

In short, *Smith*, *Miller*, *Knotts*, and *Karo*—all decided before 1985—recognized that there is no reasonable expectation of privacy in simple records voluntarily conveyed to third parties in the ordinary course of business, or in one's short-term public movements. But as new surveillance technologies "enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 585 U.S. at 305, 138 S.Ct. 2206 (quoting *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001)). Three cases illustrate that endeavor.

First, *Kyllo v. United States* held that police use of a thermal-imaging device to monitor heat waves emanating from inside a home was a search. *Kyllo*, 533 U.S. at 34–35, 121 S.Ct. 2038. The Court explained that even though the device was operated from a public street outside the home, it allowed police to "explore details of the home that would previously have been unknowable without physical intrusion." *Id.* at 40, 121 S.Ct. 2038. "Because any other conclusion would leave homeowners 'at the mercy of advancing technology,'" the Court "determined that the Government—absent a warrant—could not capitalize on such new sense-

enhancing technology to explore what was happening within the home." *Carpenter*, 585 U.S. at 305, 138 S.Ct. 2206 (quoting *Kyllo*, 533 U.S. at 35, 121 S.Ct. 2038).

Next, in *United States v. Jones*, 565 U.S. 400, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012), the Court grappled with "more sophisticated surveillance of the sort envisioned in *Knotts* and found that different principles did indeed apply." *Carpenter*, 585 U.S. at 307, 138 S.Ct. 2206. *Jones* held that the police's installation and use of a GPS tracking device to monitor the location of a suspect's vehicle for 28 days constituted a search. *Jones*, 565 U.S. at 403–04, 132 S.Ct. 945. Although Justice Scalia's opinion for the five-justice majority rested only on traditional trespass principles, five other justices authored or joined concurrences concluding that the GPS monitoring was a search under *Katz*'s reasonable-expectation-of-privacy test—even though the intrusion only captured *public* movements. *See id.* at 413–18, 132 S.Ct. 945 (Sotomayor, J., concurring); *id.* at 418–31, 132 S.Ct. 945 (Alito, J., concurring in the judgment). The concurring justices noted that, as compared to the one-trip beeper tracking in *Knotts*, the GPS tracking in *Jones* was both longer and more precise. *See id.* at 415, 132 S.Ct. 945 (Sotomayor, J., concurring); *id.* at 429–30, 132 S.Ct. 945 (Alito, J., concurring in the judgment).

Specifically, four concurring justices emphasized that long-term GPS tracking violated reasonable expectations of privacy because it enabled police to tail a suspect for much longer than would have been possible using traditional investigative methods. *See id.* at 429, 132 S.Ct. 945 (Alito, J., concurring in the judgment) ("In the pre-computer age, the greatest protections of

privacy were neither constitutional nor statutory, but practical.").

For the fifth concurring justice, Justice Sotomayor, even *short-term* GPS tracking violated reasonable expectations of privacy because it enabled such precise surveillance. *Id.* at 415, 132 S.Ct. 945 (Sotomayor, J., concurring). She reasoned that GPS technology "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* And because a short GPS search is cheaper, easier to use, and more concealable than conventional methods of surveillance, "it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" *Id.* at 416, 132 S.Ct. 945 (quoting *Illinois v. Lidster*, 540 U.S. 419, 426, 124 S.Ct. 885, 157 L.Ed.2d 843 (2004)). Moreover, GPS technology permits the Government to "store" and "efficiently mine" records of an individual's movements for "years into the future." *Id.* at 415, 132 S.Ct. 945. For these reasons, even a short GPS search could chill First Amendment freedoms and "alter the relationship between citizen and government in a way that is inimical to democratic society." *Id.* at 416, 132 S.Ct. 945 (citation omitted).[2]

---

[2] "More fundamentally," Justice Sotomayor argued, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Jones*, 565 U.S. at 417, 132 S.Ct. 945. That "approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks," without expecting their

Two years later, the Court held in *Riley v. California*, 573 U.S. 373, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014), that police must obtain a warrant to look through the contents of an arrestee's cell phone during an arrest, even though police may generally conduct brief searches of an arrestee's *person* without a warrant. *Id.* at 385–86, 134 S.Ct. 2473. The Court recognized that digital storage compiles personal information of unprecedented volume, variety, and retrospectivity into a single device (or, in the Fourth Amendment's language, "effect")—and consequently, that protecting privacy rights in such effects require a different approach. *Id.* at 393–97, 134 S.Ct. 2473.

In each of these seminal cases, the Supreme Court grappled with how to protect constitutional privacy rights from encroaching technologies. And, in the majority opinions in most of these cases and in the *Jones* concurrences, the Court recognized that then-existing Fourth Amendment case law was ill-adapted to the realities of modern technology.

B.

The Court's growing recognition of the profound impact of technological advancements on Fourth Amendment rights was on full display in its 2018 decision in *Carpenter v. United States*. While building on all that came before it, *Carpenter* marked a "sea change" in Fourth Amendment jurisprudence as it pertains to "a person's digital information." Matthew Tokson, *The*

---

devices "to enable covert surveillance of their movements." *Id.* at 417 & n.*, 132 S.Ct. 945.

Aftermath of Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 Harv. L. Rev. 1790, 1799–1800 (2022) (capitalization standardized).

In *Carpenter*, the Court held that law enforcement's request for seven days of the defendant's historical cell-site location information ("CSLI") from his wireless carrier, which produced two days' worth of data, was a search. *Carpenter*, 585 U.S. at 302, 316, 138 S.Ct. 2206. CSLI records are created when cell phones connect to nearby cell towers, which, in *Carpenter*, occurred at the start and end of the defendant's incoming and outgoing calls. *Id.* at 302, 138 S.Ct. 2206. The cell-site records were maintained by wireless carriers, which raised the possibility that the third-party doctrine would apply. And indeed, below, the Sixth Circuit had "held that [the defendant] lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers." *Id.* at 303, 138 S.Ct. 2206; *see United States v. Carpenter*, 819 F.3d 880, 888 (6th Cir. 2016). In other words, the Sixth Circuit took a view very similar to that of some of my colleagues here. *See* Judge Richardson Concurring Op., *infra*, Part II.B.

But the Supreme Court reversed. In so doing, it acknowledged that the third-party doctrine is an increasingly tenuous barometer for reasonable privacy expectations in the digital era. Instead, the Court laid the foundation for a new, multifactor test to determine when government surveillance using digital technologies constitutes a search.

Carpenter began with the *Katz* test: the Fourth Amendment protects against intrusion into the sphere in which an individual has a reasonable expectation of privacy. *Carpenter*, 585 U.S. at 304, 138 S.Ct. 2206. It then explained that, while "no single rubric" defines reasonable expectations of privacy, the Court's analysis must always be "informed by historical understandings of what was deemed an unreasonable search when the Fourth Amendment was adopted." *Id.* at 304–05, 138 S.Ct. 2206 (cleaned up). These historical understandings, according to the Court, have a few "guideposts": "the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power," "to place obstacles in the way of a too permeating police surveillance," and, most importantly, to "assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 305, 138 S.Ct. 2206 (cleaned up). The Court emphasized that in cases like *Kyllo* and *Riley*, it kept those "Founding-era understandings in mind" when considering "innovations in surveillance tools." *Id.*

Against that background, the Court quickly concluded that CSLI—"personal location information maintained by a third party"—"does not fit neatly" into any existing line of Fourth Amendment jurisprudence. *Id.* at 306, 138 S.Ct. 2206. The third-party-disclosure and public-surveillance cases could "inform [the Court's] understanding of the privacy interests at stake," but neither squarely applied. *Id.* In fact, the Court expressly "decline[d] to extend" the third-party doctrine to CSLI—even though CSLI data is maintained by third-party companies—because CSLI records are a "qualitatively different category" of information from

the phone numbers and bank records at issue in its third-party cases. *Id.* at 309, 138 S.Ct. 2206. "After all," the Court observed, "when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." *Id.* at 309, 138 S.Ct. 2206.

Instead of "mechanically applying the third-party doctrine," *id.* at 314, 138 S.Ct. 2206, *Carpenter* applied a new framework rooted in historical understandings of Fourth Amendment privacy rights but adapted to the particular surveillance technology at issue. Specifically, the Court identified four aspects of CSLI surveillance that made it "qualitatively different" from older techniques—its *comprehensiveness*, its capacity for *retrospective* tracking, the *intimacy* of the information it reveals, and its *ease of access* for police.[3] *See id.* at 309–13, 138 S.Ct. 2206. Based on those four considerations, the Court concluded that police access to CSLI violates reasonable expectations of privacy. *Id.* at 313, 138 S.Ct. 2206.

Then, in a separate section of the opinion, the Court further distinguished *Smith* and *Miller* by explaining that the conveyance of CSLI is also not meaningfully

---

[3] *Carpenter*'s framework drew on the reasoning of the *Jones* concurrences, and particularly Justice Sotomayor's concurrence. *Cf. Jones*, 565 U.S. at 415–16, 132 S.Ct. 945 (Sotomayor, J., concurring) (observing that "GPS monitoring generates a precise, comprehensive record" of "intimate information" that can be "store[d]" and "efficiently mine[d] ... for information years into the future").

voluntary. *Id.* at 313–16, 138 S.Ct. 2206. The opinion's concluding paragraph reads, in part: "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Id.* at 320, 138 S.Ct. 2206.

II.

Carpenter established a multifactor approach to assessing reasonable expectations of privacy in digital information.[4] An application of the *Carpenter* factors in

---

[4] Leading scholars agree, though they differ as to which factors are mandatory or most important. *See, e.g.*, Paul Ohm, *The Many Revolutions of* Carpenter, 32 Harv. J.L. & Tech. 357, 363, 369 (2019) (recognizing that *Carpenter* created "new, multi-factor test" to analyze an individual's reasonable privacy expectation against intruding technology and "herald[ed] a new mode of Constitutional analysis"); Susan Freiwald & Stephen W. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 Harv. L. Rev. 205, 219 (2018) (multifactor analysis was "clearly central" to the Court's holding); Tokson, *The Aftermath of* Carpenter, *supra*, at 1830 (describing the "*Carpenter* factors" and concluding from a survey of cases that "[a] multifactor *Carpenter* test has begun to emerge from the lower court[s]"); Sherwin Nam, *Bend and Snap: Adding Flexibility to the* Carpenter *Inquiry*, 54 Colum. J.L. & Soc. Probs. 131, 132 (2020) (stating that *Carpenter* "broke new ground in the constitutional right to privacy in electronic data" and employed a "five-factor" test); Helen Winters, *An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants*, 107 Minn. L. Rev. 1369, 1381, 1390 (2023) (*Carpenter* "marked a new period of Fourth Amendment jurisprudence" and laid out "several factors relevant to its decision"); Antony Barone Kolenc, *"23 and Plea": Limiting Police Use of Genealogy Sites After* Carpenter v. United States, 122 W.

this case compels the conclusion that Okello Chatrie had a reasonable expectation of privacy in his Location History data.[5]

A.

Carpenter first considered the comprehensiveness of CSLI data, observing that it "tracks nearly exactly the movements of [a cell phone's] owner," providing "an all-encompassing record of the holder's whereabouts." *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206. Unlike a vehicle, "a cell phone—almost a 'feature of human anatomy'— ... faithfully follows its owner beyond public thoroughfares and into private residences, doctor's

---

Va. L. Rev. 53, 71–72 (2019) (concluding that *Carpenter* "alter[ed] Fourth Amendment law" by recognizing a privacy interest in the "whole of a person's physical movements," and "balanced five factors" to analyze that interest); Matthew Tokson, *The* Carpenter *Test as a Transformation of Fourth Amendment Law*, 2023 U. Illinois L. Rev. 507, 517–20 (2023) (outlining a three-factor test); Allie Schiele, *Learning from Leaders: Using* Carpenter *to Prohibit Law Enforcement Use of Mass Aerial Surveillance*, 91 Geo. Wash. L. Rev. Arguendo 14, 17–18 (2023) (pointing out "*Carpenter*'s focus on five central factors"); Nicole Mo, *If Wheels Could Talk: Fourth Amendment Protections Against Police Access to Automobile Data*, 98 N.Y.U. L. Rev. 2232, 2251 (2023) (recognizing factors); Luiza M. Leão, *A Unified Theory of Knowing Exposure: Reconciling* Katz *and* Carpenter, 97 N.Y.U. L. Rev. 1669, 1684 (2022) (same); Matthew E. Cavanaugh, *Somebody's Tracking Me: Applying Use Restrictions to Facial Recognition Tracking*, 105 Minn. L. Rev. 2443, 2468 (2021) (same).

[5] Police obtained *Chatrie's* Location History data when they obtained Location History data that was traceable to *him*. Here—as Judge Berner persuasively explains—that happened at Step 2 of Google's three-step process. *See* Judge Berner Concurring Op., *infra*, Part II.B.i.

offices, political headquarters, and other potentially revealing locales." *Id.* (quoting *Riley*, 573 U.S. at 385, 134 S.Ct. 2473).

Like CSLI, Location History tracks a smartphone's location—only more precisely. CSLI (as described in *Carpenter*) places a user within a "wedge-shaped sector," *id.* at 312, 138 S.Ct. 2206, ranging from "a dozen" to "several hundred" city blocks in size, which can be "up to 40 times more imprecise" in rural areas, *id.* at 324, 138 S.Ct. 2206 (Kennedy, J., dissenting). But Location History can locate a user within *meters*—and can even measure elevation, identifying the specific floor in a building where a person might be. *United States v. Chatrie*, 590 F. Supp. 3d 901, 908–09 (E.D. Va. 2022). Moreover, the CSLI collected in *Carpenter* was only recorded when a user placed or received a call—no call, no data. *Carpenter*, 585 U.S. at 302, 138 S.Ct. 2206. But Location History tracks a user's location *automatically*, every *two minutes*. *Chatrie*, 590 F. Supp. 3d at 908. In *Carpenter*, law enforcement collected only about 101 CSLI data points in a full day. *Carpenter*, 585 U.S. at 302, 138 S.Ct. 2206. Here, police were able to collect an average of about 76 Location History data points on each person surveilled in just *two hours*. *See* J.A. 1121 (explaining that "Google produced ... a total of 680 data points" for "nine accounts" at Step 2). If CSLI as described in *Carpenter* enables "near perfect surveillance," *Carpenter*, 585 U.S. at 312, 138 S.Ct. 2206, so too does Location History.

B.

Carpenter next considered "the retrospective quality of [CSLI] data," which (at the time) was "continually logged for all of the 400 million devices in the United States" and retained by wireless carriers "for up to five years." *Carpenter*, 585 U.S. at 312, 138 S.Ct. 2206. CSLI allowed police to "travel back in time" to "reconstruct a person's movements," unlocking "a category of information otherwise unknowable." *Id.* And because CSLI tracking "runs against everyone," "police need not even know in advance whether they want to follow a particular individual, or when." *Id.* "Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years." *Id.*

Location History data raises similar concerns. Google begins collecting Location History the moment the feature is enabled and retains it indefinitely, enabling police to retrospectively tail a suspect with remarkable precision.[6] And like CSLI, police need not identify the suspect in advance—Location History data is available for "numerous tens of millions" of Google users. *Chatrie*, 590 F. Supp. 3d at 907. Of course, a geofence limits the size and duration of any particular law enforcement data-grab. But *Carpenter*'s retrospectivity analysis emphasized the vast scope of *available* CSLI data, which gives police "*access* to a category of information otherwise unknowable." *Carpenter*, 585 U.S. at 312, 138 S.Ct. 2206 (emphasis added). So too here.

---

[6] This discussion reflects the record in this case, not Google's current or future practices.

In fact, Location History permits even broader surveillance than CSLI. Collecting CSLI data at least requires police to produce a suspect's phone number in order to access a five-year trove of their location data. But a geofence can uncover the Location History of an unlimited number of individuals, *none* of whom were previously identified or suspected of any wrongdoing. Indeed, the very point of a geofence is to generate leads where none exist.[7] Consequently, *Carpenter*'s concerns about retrospective surveillance apply to Location History with even greater force.

C.

Carpenter further concluded that "time-stamped [location] data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206 (quoting *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (Sotomayor, J.,

[7] This feature of geofence warrants makes them uncomfortably akin to the "reviled" general warrants that the Framers intended the Fourth Amendment to forbid. *Carpenter*, 585 U.S. at 303, 138 S.Ct. 2206 (quoting *Riley*, 573 U.S. at 403, 134 S.Ct. 2473); *see United States v. Smith*, 110 F.4th 817, 836–38 (5th Cir. 2024). "The general warrant specified only an offense ... and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220, 101 S.Ct. 1642, 68 L.Ed.2d 38 (1981). As Judge Berner explains, probable cause may support a tightly limited geofence warrant. *See* Judge Berner Concurring Op., *infra*, Part II.D. But if accessing Location History is not a search at all, police would not even need to specify an offense before dipping into years of personal location data on millions of Americans.

concurring)). Such "location records," the Court recognized, "hold for many Americans the privacies of life." *Id.* (quoting *Riley*, 573 U.S. at 403, 134 S.Ct. 2473).

The same is true of Location History. The two hours of geographically unbounded data requested by police at Step 2 illustrate that "the potential intrusiveness of even a snapshot of precise location data should not be understated." *United States v. Smith*, 110 F.4th 817, 833 (5th Cir. 2024). The geofence in this case centered on "a busy part of the Richmond metro area" between 3:50 and 5:50 p.m., when many people are leaving work or school—and of course, it had no geographic boundaries at Step 2. *Chatrie*, 590 F. Supp. 3d at 925; *see id.* at 919. Two hours of Location History for accounts passing through that geofence could enable police to tour a person's home, capture their romantic rendezvous, or accompany them to church.

This case presents textbook examples of how police access to this digital information can invade the privacies of innocent users. At the suppression hearing, Chatrie's counsel demonstrated that the anonymized Step 2 data produced in response to this geofence warrant tracked three innocent users to or from private spaces, including residences, a school, and a hospital. *Id.* at 923–24. Chatrie's expert showed how this information, when combined with publicly available information, allowed him to easily deduce those individuals' identities. *Id.*[8]

---

[8] Whether the Location History collected here placed Chatrie himself inside a constitutionally protected space is beside the point. "In *Carpenter*, the Supreme Court's analysis of whether the

Some of my colleagues believe that because a two-hour snippet of Location History is too short to "reveal intimate details through habits and patterns," like the aerial surveillance footage in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330, 341 (4th Cir. 2021), it cannot reveal intimate details at all. *See* Judge Richardson Concurring Op., *infra*, at 140 n.19. But pattern-based deductions are not the *only* way

---

Government's access of the defendant's CSLI impeded his reasonable expectation of privacy was *not* based on a review of the specific results of the search in that case." *United States v. Smith*, 110 F.4th 817, 834 n.8 (5th Cir. 2024) (citing *Carpenter*, 585 U.S. at 309–13, 138 S.Ct. 2206). Instead, "[t]he question was whether the technology utilized by law enforcement had the *capability* of providing data that offered 'an all-encompassing record of [a person's] whereabouts,' regardless of whether that person actually entered spaces that are traditionally considered protected under the Fourth Amendment." *Id.* (quoting *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206).

Similarly, *Kyllo* rejected the argument that the search of heat waves emanating from a home did not implicate the Fourth Amendment if the search did not reveal intimate details. That argument, Justice Scalia explained, was not only "wrong in principle," but also "impractical" because "no police officer would be able to know in advance whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." *Kyllo*, 533 U.S. at 38–39, 121 S.Ct. 2038. Likewise, when police drew up a geofence that included private spaces, they could not predict whether Chatrie would be shown to have entered those spaces. The Government cannot circumvent the Constitution merely because, by sheer luck, its target did not stray from the safe zone. *See Arizona v. Hicks*, 480 U.S. 321, 325, 107 S.Ct. 1149, 94 L.Ed.2d 347 (1987) ("A search is a search, even if it happens to disclose nothing but the bottom of a turntable.").

to uncover intimate personal details.[9] Another way is to use a surveillance technology that can follow subjects through walls. *See Kyllo*, 533 U.S. at 37–39, 121 S.Ct. 2038. The aerial surveillance program at issue in *Beautiful Struggle* tracked only *public* movements, so our short-term–long-term distinction made sense; it takes a lot of grainy aerial footage to deduce intimate personal details.[10] Location History's accuracy—not to mention its vast retrospective scope—makes it a much more potent tool.

A few of my colleagues claim that "[a] record of a person's single, brief trip is no more revealing than his bank records or telephone call logs." Judge Richardson Concurring Op., *infra*, at 140. Respectfully, that is wrong on multiple accounts. Most obviously, it flat-out ignores the public surveillance doctrine. Tracking a person's "single, brief trip" on public thoroughfares (as in *Knotts*) is not a search; but tracking even an *object*'s trip in and out of a private space (as in *Karo*) *is* a search. *Compare Knotts*, 460 U.S. at 281, 103 S.Ct. 1081 *with Karo*, 468 U.S. at 714–16, 104 S.Ct. 3296. Location History is capable of tracking *people* in and out of private spaces, with even greater precision than CSLI or the

---

[9] Indeed, *Carpenter* made no mention of habits or patterns in discussing the capabilities of CSLI.

[10] The weeks-long aerial surveillance program at issue in *Beautiful Struggle* monitored only public spaces during the day, gathered hours-long chunks of image data in which people appeared as blurry collections of pixels, and stored that data for forty-five days. *Beautiful Struggle*, 2 F.4th at 334, 341–42. As a result, the Government had to decipher individuals' identities from several pieces of captured data. *Id.* at 344–45.

beeper in *Karo*. More tellingly, *Carpenter* expressly recognized that the deeply revealing nature of "cell phone location records" puts them in a "qualitatively different category" from "telephone numbers and bank records." *Carpenter*, 585 U.S. at 309, 138 S.Ct. 2206. *Carpenter*'s observation about CSLI is doubly true of Location History.

In light of the intimately revealing nature of Location History data, the span of time it covers is of little importance to the Fourth Amendment search analysis. The Government in *Carpenter* requested CSLI spanning both seven- and 152-day periods, which revealed, respectively, two and 127 days of data. *Id.* at 302, 138 S.Ct. 2206. But *Carpenter* ultimately held that accessing the shorter span of data was enough to constitute a Fourth Amendment search. *Id.* at 310 n.3, 138 S.Ct. 2206. The Court's intimacy analysis drew on Justice Sotomayor's concurrence in *Jones*, which argued that even *short-term* GPS tracking violates reasonable expectations of privacy. *See id.* at 311, 138 S.Ct. 2206 (citing *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (Sotomayor, J., concurring)).

Moreover, *Carpenter* focused on the nature of the search technology employed, not the duration of the particular search at bar. Even though the Government only accessed discrete segments of Carpenter's CSLI, the Court stressed repeatedly that carriers collect and store CSLI for "years." *Id.* at 312, 313, 315, 319, 138 S.Ct. 2206. Location History collects even more (and more precise) location data, and stores it indefinitely. Applying *Carpenter*'s logic, police use of a technology whose very purpose is to generate a dossier of intimately revealing

location data traceable to individuals is a search—even if only a snippet is ultimately obtained.

At bottom, focusing on the duration of the geofence employed in this particular case "overlooks the critical issue": that Location History "is an entirely different species of business record[,] something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers." *Id.* at 318, 138 S.Ct. 2206. There can be no doubt that even a small amount of such data "provides an intimate window into a person's life." *Id.* at 311, 138 S.Ct. 2206.

D.

Carpenter also found it significant that CSLI searches are "easy, cheap, and efficient compared to traditional investigative tools." *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206. That concern echoes the *Jones* concurrences, which warned that low-cost surveillance technologies could lead to more surveillance and less accountability. Justice Sotomayor's concurrence noted that "because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" *Jones*, 565 U.S. at 415–16, 132 S.Ct. 945 (Sotomayor, J., concurring) (quoting *Lidster*, 540 U.S. at 426, 124 S.Ct. 885). And Justice Alito added that GPS technology "makes long-term monitoring"—which was traditionally "difficult and costly and therefore rarely undertaken"—

"relatively easy and cheap." *Id.* at 429, 132 S.Ct. 945 (Alito, J., concurring in the judgment).

Location History is like the GPS monitoring in *Jones*, only cheaper and more intrusive. Scholars have estimated that "tracking location by cell phone," as police did in *Carpenter*, "is almost twice as cheap as GPS tracking," which in turn is "twenty-eight times cheaper than covert pursuit." Ohm, *supra* n.4, at 369 (citing Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. Online 335, 354 (2014)). Location History tracking is likely even cheaper. "With just the click of a button," Google—at the Government's request—"can access [its] deep repository of historical location information at practically no expense" to the Government. *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206. And unlike the tracking device in *Jones*, which followed the suspect's Jeep on public roads, *see Jones* 565 U.S. at 403, 132 S.Ct. 945, Location History "follows its [subject] beyond public thoroughfares" and into private spaces, *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206.

Plainly, Location History monitoring is vastly cheaper and easier to deploy than traditional investigative tools. It permits police to access private location data far more often and much more inconspicuously than the surveillance technologies that have shaped society's reasonable expectations of privacy.

* * *

In sum, all four considerations that led *Carpenter* to conclude that "when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy" apply with equal or greater force here. Thus, when the Government accessed Location History data that was traceable to Chatrie, it invaded his reasonable expectation of privacy.

III.

The Government—along with a few of my colleagues—would prefer to resolve this case by "mechanically applying the third-party doctrine," *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206. They contend that Chatrie lacked any reasonable expectation of privacy in his Location History because he voluntarily conveyed that data to Google.

That argument is several decades beyond its time. In *Carpenter*, the Government argued that police access to CSLI was simply "a garden-variety request for information from a third-party witness." *Id.* at 313, 138 S.Ct. 2206. But *Carpenter* rejected that simplistic, outdated approach because it "fail[ed] to contend with the seismic shifts in digital technology that made [detailed location tracking] possible." *Id.* We should do the same here.

Carpenter's Fourth Amendment search analysis proceeded in two parts. Part III.A. of the Court's opinion considered the comprehensiveness, retrospectivity, intimacy, and efficiency of CSLI tracking and concluded that police access to such data

violated Carpenter's reasonable expectation of privacy. *Id.* at 310–13, 138 S.Ct. 2206. The next section, Part III.B., addressed voluntariness—the Government's argument that Carpenter's disclosure of CSLI to his wireless carrier undermined that expectation.[11] *Id.* at 313–16, 138 S.Ct. 2206. The Court flatly rejected that argument for two reasons, both of which apply here.

A.

First, the Court explained that "the revealing nature of CSLI" records put them in a "distinct category of information" from the kinds of documents to which the third-party doctrine has been applied. *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206. The Court in the 1979 case of *Smith*, for instance, stressed the "limited capabilities" of a pen register: it does "not acquire the *contents* of communications," nor reveal the caller and call recipient's "identities, nor whether the call was even completed." *Smith*, 442 U.S. at 741–42, 99 S.Ct. 2577 (citation omitted). And the 1976 case of *Miller* emphasized that the suspect's bank records were not

[11] Several scholars have noted that *Carpenter*'s discussion of voluntariness in a separate rebuttal section suggests that it is the least important factor in the overall analysis—if indeed it is properly considered a factor at all. *See* Matthew Tokson, *Smart Meters as a Catalyst for Privacy Law*, 72 Fla. L. Rev. Forum 104, 112 (2022) ("Most scholars view involuntariness not as a requirement but as merely one factor among many examined in *Carpenter*. The Court's discussion of the voluntariness issue ... was mostly confined to a single paragraph in a lengthy opinion that largely focused on [other] factors[.]" (footnote omitted) (collecting sources)); Freiwald & Smith, *supra* n.4, at 219 (observing that *Carpenter* established a test made up of only the four factors discussed above).

"private papers" or "confidential communications but negotiable instruments to be used in commercial transactions." *Miller*, 425 U.S. at 440, 442, 96 S.Ct. 1619. But in 2018, the *Carpenter* Court saw "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." *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206.

So too here in 2025. As already discussed at length, Location History is at least as comprehensive, retrospective, intrusive, and efficient a technology as CSLI. Like CSLI, Location History is "compiled every day, every moment, over several years." *Id.* at 314–15, 138 S.Ct. 2206. It can provide "not just dialed digits, but a detailed and comprehensive record of [a] person's movements." *Id.* at 309, 138 S.Ct. 2206. And it is "effortlessly compiled," accessible at "the click of a button" and "at practically no expense." *Id.* at 309, 311, 138 S.Ct. 2206.

Most fundamentally, what sets CSLI and Location History apart from bank records and phone logs is that they concern a person's physical movements. *Carpenter* recognized that the *Jones* concurrences—representing the views of five justices—reflect a "special solicitude for location information in the third-party context." *Id.* at 314, 138 S.Ct. 2206. The *Carpenter* majority endorsed that concern, expressly acknowledging that CSLI's capacity to track a person's "physical presence" naturally "implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Id.* at 315, 138 S.Ct. 2206. The same is true of Location History.

B.

Second, *Carpenter* recognized that cell phone users do not, in any "meaningful sense," "voluntarily assume the risk of turning over a comprehensive dossier of [their] physical movements." *Carpenter*, 585 U.S. at 315, 138 S.Ct. 2206 (cleaned up). The Court began with the premise that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.* at 315, 138 S.Ct. 2206 (quoting *Riley*, 573 U.S. at 385, 134 S.Ct. 2473). And "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." *Id.* at 315, 138 S.Ct. 2206.[12] Unlike the bank records and phone numbers in *Smith* and *Miller*, which were conveyed to companies by customers' physical, affirmative acts, the collection of CSLI is "inescapable and automatic," such that a cell phone user has "no way to avoid leaving behind a trail of location data." *Id.* at 315, 320, 138 S.Ct. 2206.

---

[12] Although the CSLI data at issue in *Carpenter* was only collected at the start and end of calls, the Court recognized that "in recent years," companies had also begun collecting CSLI "from the transmission of text messages and routine data connections," resulting in "increasingly vast amounts of increasingly precise CSLI." *Carpenter*, 585 U.S. at 301, 138 S.Ct. 2206. Accordingly, the Court considered not only CSLI's present capacities, but its emerging potential. *See id.* at 313, 138 S.Ct. 2206 (recognizing that "the rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'" (quoting *Kyllo*, 533 U.S. at 36, 121 S.Ct. 2038)).

Sharing Location History—while admittedly not wholly "inescapable"—is not meaningfully voluntary either. Most importantly, Location History is just one example of a category of personal data–driven services that have become "indispensable to participation in modern society." *Id.* at 315, 138 S.Ct. 2206. Nine in ten Americans own a smartphone, [13] and countless smartphone apps rely on users' personal data for both functionality and revenue. Consequently, Americans face enormous pressure to entrust detailed personal information to third parties in exchange for services. Tens of millions of citizens "opt" into services that collect and store years' worth of intimate information—including location history, medical records, financial data, family photos, private communications, and more—on remote servers managed by private corporations. Some of these services are simply convenient; others are mandated by employers; still others may be critical to a user's health or safety. Location History is a particularly useful and widely adopted example, used by "numerous tens of millions" for everyday services like traffic updates. *Chatrie*, 590 F. Supp. 3d at 907.

None of this means that Americans have ceded a reasonable expectation of privacy in their detailed private information. Smartphone users might reasonably expect that their deidentified data will be used, in aggregate, to fine-tune targeted advertising. But it would be a grave misjudgment to conflate an

---

[13] *Mobile Fact Sheet*, Pew Rsch. Ctr. (Nov. 13, 2024), https://www.pewresearch.org/internet/fact-sheet/mobile [https://perma.cc/QQ7M-WWLP].

individual's limited disclosure to Google with an open invitation to the state. *See Jones*, 565 U.S. at 418, 132 S.Ct. 945 (Sotomayor, J., concurring) ("I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."); *Smith*, 442 U.S. at 749, 99 S.Ct. 2577 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").

Of course, Location History has to be enabled—and on this slim reed rests the bulk of the Government's case. But opting into Location History communicates less about a customer's expectations of privacy than the Government would have us believe. "As anyone with a smartphone can attest, electronic opt-in processes are hardly informed and, in many instances, may not even be voluntary. Google's Location History opt-in process is no different." *United States v. Smith*, 110 F.4th 817, 835–36 (5th Cir. 2024) (citations omitted).

Approving a lucrative location-tracking feature on a smartphone is frictionless by design. Here, the record indicates that Location History can be enabled within a few moments of setting up and using an Android device like the one Chatrie used. One of the first steps in setting up a smartphone that runs on Android is to log into or create a Google account, a prerequisite for access to many of the smartphone's features, such as downloading apps, accessing Google Maps, or syncing Google services

like Calendar and Contacts. The district court found that Google repeatedly prompts its millions of Android users to opt-in to Location History both upon initial set-up and then "multiple times across multiple apps." *Chatrie*, 590 F. Supp. 3d at 909; *see* J.A. 128–29.

As the district court recognized, Google's privacy warnings and descriptive pop-ups are "limited," "partially hidden," and "less than pellucid." *Chatrie*, 590 F. Supp. 3d at 936. The pop-up text that appears when Google prompts users to opt in explains only that Location History "[s]aves where you go with your devices," and that "[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com." *Id.* at 911–12. Below that, the screen provides the options: "NO THANKS" or a brightly highlighted "TURN ON." *Id.* at 912. It also presents a small expansion arrow, which, if tapped, displays more information about Location History.[14] But a user does not need to click the expansion arrow to opt into Location History. They can just click "TURN ON." Through that single tap, Location History is enabled. *See id.*

---

[14] The expansion arrow reveals the following additional information: "Location History saves where you go with your devices. To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, like Google Maps or Search.... This data may be saved and used in any Google service where you were signed in to give you more personalized experiences." *Chatrie*, 590 F. Supp. 3d at 912.

At the time Chatrie enabled Location History, this pop-up copy "did not detail ... how frequently Google would record [his] location ...; the amount of data Location History collects (essentially *all* location information); that even if he 'stopped' location tracking it was only 'paused' ...; or, how precise Location History can be." *Id.* at 936. It did not explain that Location History would automatically and precisely track his location even when he wasn't using his phone—and would continue even if he deleted the Google app through which he enabled it. *See id.* at 909. Nor did it explain that Location History would track his location on all of his Google-connected devices—not just those on which he enabled the feature. *Id.* at 909. It certainly didn't warn him that *police* could access his location data. *Cf. Jones*, 565 U.S. at 417 n.*, 132 S.Ct. 945 (Sotomayor, J., concurring) ("[S]mart phone[ ] [owners] do not contemplate that these devices will be used to enable covert surveillance of their movements.").

Moreover, once a user has opted into Location History, opting out is easier said than done. "Pausing" Location History "halts the collection of future data," but "*does not delete* information Google has already obtained." *Chatrie*, 590 F. Supp. 3d at 912 (quoting J.A. 778). And the record reflects that misleading pop-ups try to dissuade users from pausing the service by suggesting that various Google apps need Location History in order to function properly. *Id.* at 913. These pop-ups "do[ ] not specifically detail how app functionality might be limited"; and in fact, most apps "will, indeed, continue to function without Location History enabled." *Id.*

At the time Chatrie enabled Location History, a user could only *delete* their Location History through Google's web browser–based "Timeline" feature. *See id.* at 913. One Google employee familiar with that process remarked in an email that it "*feels* like it is designed to make [deleting Location History] *possible*, yet *difficult* enough that people won't figure [it] out." *Id.* (quoting J.A. 1631). Around the time Chatrie enabled the feature, Google faced criticism from members of Congress, the media, and Norway's Consumer Protection Committee for the lack of transparency in how users enable or disable Location History. *See id.* at 909 n.11, 913 & n.16.

In short, the single tap required to enable Location History does not represent a user's well-informed or meaningfully voluntary disclosure of "a comprehensive dossier of his physical movements." *Carpenter*, 585 U.S. at 315, 138 S.Ct. 2206. "Although, unlike in *Carpenter*, Chatrie apparently took some affirmative steps to enable location history, those steps likely do not constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day.... a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting 'YES, I'M IN' at midnight while setting up Google Assistant, even if some text offered warning along the way." *Chatrie*, 590 F. Supp. 3d at 936.[15]

---

[15] Some of my colleagues argue that this single tap sets Location History apart from CSLI, such that *Carpenter*'s reasoning does not apply here. *See* Judge Richardson Concurring Op., *infra*, at 139–41. But the proper comparison in a voluntary-disclosure analysis is not

* * *

In sum, the third-party doctrine is wholly inadequate to defeat Chatrie's reasonable expectation of privacy in Location History data traceable to him. Chatrie—like tens of millions of Americans—shared that data with Google in exchange for widely used services. But that "does not mean that the Fourth Amendment falls out of the picture entirely.'" *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206 (quoting *Riley*, 573 U.S. at 392, 134 S.Ct. 2473). Location History—like CSLI—enables comprehensive, retrospective, intimate, and highly efficient surveillance. Accordingly, "the fact that the Government obtained the information from a third party does not overcome [Chatrie's] claim to Fourth Amendment protection." *Id.* at 315–16, 138 S.Ct. 2206. The Government's acquisition of Chatrie's Location

---

to CSLI, but to the bank and phone records in *Smith* and *Miller*. In *Smith*, the individuals under surveillance physically dialed each number police obtained, and the phone company sent monthly bills listing some of the calls that the companies had collected. *Smith*, 442 U.S. at 742, 99 S.Ct. 2577 (noting that users "see a list of their long-distance (toll) calls on their monthly bills"). And in *Miller*, which was decided before the advent of online banking, the suspects physically brought the checks and deposit slips at issue to the bank. *Miller*, 425 U.S. at 442, 96 S.Ct. 1619.

By contrast, once enabled, Location History collects its data inconspicuously and automatically, "without any affirmative act on the part of the user." *Carpenter*, 585 U.S. at 315, 138 S.Ct. 2206. A feature that silently documents one's physical location every two minutes—even if enabled with a single tap, years ago, in exchange for traffic updates—is not remotely comparable to the kinds of voluntary disclosures that have been found to undermine reasonable expectations of privacy under the third-party doctrine.

History "was a search within the meaning of the Fourth Amendment." *Id.* at 316, 138 S.Ct. 2206.

IV.

Today, the Court declines to decide whether law enforcement may access Location History data without a warrant. In doing so, it leaves unresolved a question of immense constitutional significance: whether the Government may track a person's movements—potentially for weeks or months—without judicial oversight. That uncertainty threatens not only Chatrie's privacy, but the privacy of all Americans.

Instead of addressing that compelling constitutional issue, this Court takes refuge in the good-faith exception—and thereby clears the path for widespread, surreptitious police surveillance. The result is plain. It leaves the door open for law enforcement to monitor religious services, political protests, gun shows, union meetings, or AA sessions—all without a warrant, all without judicial oversight or accountability. The technology at issue here does not merely capture a person's location at a single moment; it allows the Government to "reconstruct a person's movements." *Carpenter*, 585 U.S. at 312, 138 S.Ct. 2206. At a minimum, requiring a warrant to obtain such data is necessary to preserve the Fourth Amendment's protections.

Unchecked police surveillance "alter[s] the relationship between citizen and government in a way that is inimical to democratic society." *Jones*, 565 U.S. at 416, 132 S.Ct. 945 (Sotomayor, J., concurring) (citation omitted). A

broad range of associational and expressive freedoms—private conversations, peaceful assembly, investigative journalism—can be chilled by the knowledge "that the Government may be watching." *Id.* "The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide." *Smith*, 442 U.S. at 751, 99 S.Ct. 2577 (Marshall, J., dissenting).[16]

Limiting law enforcement's access to powerful surveillance technologies "is not costless. But our rights are priceless. Reasonable minds can differ, of course, over the proper balance to strike between public interests and individual rights." *United States v. Smith*, 110 F.4th 817, 841 (5th Cir. 2024) (Ho, J., concurring). But the Court's unwillingness to confront that question head-on falls short of our duty. The Fourth Amendment demands more.

---

[16] Ironically, decisions like this one could also hinder legitimate law enforcement efforts. Shortly after the first oral argument in this case, Google—apparently predicting the panel majority's flawed reading of *Carpenter*—announced its intention to stop centrally storing users' Location History data, thereby reducing the potential for legitimate investigatory uses of Location History data, even with a warrant. *See* Cyrus Farivar & Thomas Brewster, *Google Just Killed Warrants That Give Police Access to Location Data*, Forbes (Dec. 14, 2023), https://www.forbes.com/sites/cyrusfarivar/2023/12/14/google-just-killed-geofence-warrants-police-location-data [https://perma.cc/GCP9-QPBG].

RICHARDSON, Circuit Judge, with whom WILKINSON, NIEMEYER, KING, AGEE, QUATTLEBAUM, and RUSHING, Circuit Judges, join, concurring:

Okello Chatrie appeals the district court's denial of his motion to suppress location data obtained using a geofence warrant. He argues that the geofence warrant violated the Fourth Amendment because it lacked probable cause and particularity. But obtaining just two hours of location information that was voluntarily exposed is not a Fourth Amendment search and therefore doesn't require a warrant at all. I would therefore affirm Chatrie's conviction.

I. Background

This case involves government access to a specialized form of location information maintained by Google. Understanding the nature of this information, how it is generated, and how Google obtains it is necessary to understand why the third-party doctrine applies. Accordingly, I begin with a description of the relevant technology.[1]

---

[1] Google has announced changes to its Location History setting. *See* Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, Google (Dec. 12, 2023), [https://perma.cc/Y62G-GBUW]. The following description of the facts reflects the record in this case, not Google's technology and practices now or in the future.

A. Google Location History and Geofence Warrants

Few readers need an introduction to Google, the technology supergiant that offers products and services like Android, Chrome, Google Search, Maps, Drive, and Gmail. This case, however, is about a particular setting for mobile devices that Google calls "Location History."

Location History is an optional account setting that allows Google to track a user's location while he carries his mobile devices. If a user opts in, Google keeps a digital log of his movements and stores this data on its servers. Google describes this setting as "primarily for the user's own use and benefit." J.A. 131. And enabling it does unlock several useful features for a user. For instance, he can view a "virtual journal" of his past travels in the "Timeline" feature of the Google Maps app. J.A. 128. He can also obtain personalized maps and recommendations, find his phone if he loses it, and receive real-time traffic updates. But Google uses and benefits from a user opting in, too—mostly in the form of advertising revenue. Google uses Location History to show businesses whether people who viewed an advertisement visited their stores. It similarly allows businesses to send targeted advertisements to people in their stores' proximity.

Location History is turned off by default, so a user must take several affirmative steps before Google begins tracking and storing his Location History data. First, he

must enable location sharing on his mobile device.[2] Second, he must opt in to the Location History setting on his Google account, either through an internet browser, a Google application (such as Google Maps), or his device settings (for Android devices). Before he can activate the setting, however, Google always presents him language that explains the basics of the service.[3] Third, he must enable the "Location Reporting" feature on his mobile device.[4] And fourth, he must sign in to his Google account on that device. Only when a user follows these steps will Google begin tracking and storing his Location History data. Roughly one-third of active Google users have enabled Location History.

Even after a user opts in, he maintains some control over his location data. He can review, edit, or delete any information that Google has already obtained. So, for

---

[2] For iOS devices, he must also grant location permission to applications capable of using that information.

[3] This text is the same no matter how a user opts in to Location History. It explains that Location History "[s]aves where you go with your devices," and that "[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change it in your settings at account.google.com." J.A. 1564. It also presents an expansion arrow, which, if tapped by the user, displays more information about Location History. For instance, it explains that "Google regularly obtains location data from your devices ... even when you aren't using a specific Google service." J.A. 1565.

[4] Location Reporting allows a user to control which devices in particular will generate Location History information. So a user could enable Location History at the account level but then disable Location Reporting for a particular device. That device then would not generate Location History data.

instance, he could decide he only wants to keep data for certain dates and to delete the rest. Or he could decide to delete everything. Google also allows him to pause (*i.e.*, disable) the collection of future Location History data.[5] Whatever his choice, Google will honor it. From start to finish, then, the user controls how much Google tracks and stores his Location History data.

Once a user enables Location History, Google constantly monitors his location through GPS, even when he isn't using his phone.[6] And if he has an Android phone, he can turn on another setting—"Google Location Accuracy"—that enables Google to determine his location using more inputs than just GPS, such as Wi-Fi access points and mobile networks. As a result, Location History can be more precise than other location-tracking mechanisms, including cell-site location information. But whether Google Location Accuracy is activated or not, Location History's power should not be exaggerated. In the end, it is only an estimate of a device's location. So when Google records a set of location coordinates, it includes a value (measured in meters) called a "confidence interval," which represents Google's confidence in the accuracy of the estimate.[7] Google represents that for

---

[5] Additionally, if a user disables location sharing on his device, that device will cease sharing location information with Location History, even if Location History and Location Reporting remain enabled.

[6] On average, Google logs a device's location every two minutes.

[7] For example, if the confidence interval is one hundred meters, then Google estimates that a user is likely within a one-hundred-meter radius of the coordinates.

any given location point, there is a 68% chance that a user is somewhere within the confidence interval.

Google stores all Location History data in a repository called the "Sensorvault." The Sensorvault assigns each device a unique identification number and maintains all Location History data associated with that device. Google then uses this data to build aggregate models to assist applications like Google Maps.

In 2016, Google began receiving "geofence warrants" from law enforcement seeking to access location information. A geofence warrant requires Google to produce Location History data for all users who were within a geographic area (called a geofence) during a particular time period.[8] Since 2016, geofence requests have skyrocketed: Google claims it saw a 1,500% increase in requests from 2017 to 2018 and a 500% increase from 2018 to 2019. Concerned with the potential threat to user privacy, Google consulted internal counsel and law enforcement agencies in 2018 and developed its own three-step procedure for responding to geofence requests. Since then, Google has objected to any geofence request that disregards this procedure.

Google's procedure works as follows: At Step One, law enforcement obtains a warrant that compels Google to disclose an anonymous list of users whose Location History shows they were within the geofence during a specified timeframe. But Google does not keep any lists

---

[8] Geofence warrants seek only Location History data and no other forms of location information, so they only affect people who had this feature enabled at the requested time and place.

like this on hand. So it must first comb through its entire Location History repository to identify users who were present in the geofence. Google then gives law enforcement a list that includes for each user an anonymized device number, the latitude and longitude coordinates and timestamp of each location point, a confidence interval, and the source of the stored Location History (such as GPS or Wi-Fi). Before disclosing this information, Google reviews the request and objects if Google deems it overly broad.

At Step Two, law enforcement reviews the information it receives from Google. If it determines that it needs more, then law enforcement can ask Google to produce additional location coordinates. This time, the original geographical and temporal limits no longer apply; for any user identified at Step One, law enforcement can request information about his movements inside and outside the geofence over a broader period. Yet Google generally requires law enforcement to narrow its request for this more expansive location data to only a subset of the users pinpointed in Step One.

Finally, at Step Three, law enforcement determines which individuals are relevant to the investigation and then compels Google to provide their account-identifying information (usually their names and email addresses). Here, too, Google typically requires law enforcement to taper its request from the previous step, so law enforcement can't merely request the identity of every user identified in Step Two.

B. Facts

On May 20, 2019, someone robbed the Call Federal Credit Union in Midlothian, Virginia. The suspect carried a gun and took $195,000 from the bank's vault. He then fled westward before police could respond.

The initial investigation into the robbery proved unfruitful. When Detective Joshua Hylton arrived at the scene, he interviewed witnesses and reviewed the bank's security footage. But these failed to reveal the suspect's identity. And after chasing down two dead-end leads, Detective Hylton seemed to be out of luck.

Yet there was one thing Detective Hylton still hadn't tried. He saw on the security footage that the suspect had carried a cell phone during the robbery. In the past, Detective Hylton had sought and obtained three separate geofence warrants after consulting prosecutors. So on June 14, 2019, he applied for and obtained a geofence warrant from the Chesterfield County Circuit Court of Virginia.

The warrant drew a geofence with a 150-meter radius covering the bank. It then laid out the three-step process by which law enforcement would obtain location information from Google. At Step One, Google would provide anonymized Location History information for all devices that appeared within the geofence from thirty minutes before to thirty minutes after the bank robbery. This information would include a numerical identifier for each account. At Step Two, law enforcement would "attempt[ ] to narrow down that list" to a smaller number of accounts and provide the narrowed list to

Google. J.A. 116. Google would then disclose anonymized location data for all those devices from one hour before to one hour after the robbery. But unlike the Step One information, the Step Two information would be unbounded by the geofence. Finally, at Step Three, law enforcement would again attempt to shorten the list, and Google would provide the username and other identity information for the requested accounts.

In response to the warrant, Google first provided 209 location data points from nineteen accounts that appeared within the geofence during the hour-long period. Detective Hylton then requested Step Two information from nine accounts identified at Step One. Google responded by producing 680 data points from these accounts over the two-hour period. Finally, Detective Hylton requested the subscriber information for three accounts, which Google provided. One of these accounts belonged to Okello Chatrie.[9]

C. Procedural History

On September 17, 2019, a grand jury in the Eastern District of Virginia indicted Chatrie for (1) forced accompaniment during an armed credit union robbery, in violation of 18 U.S.C. §§ 2113(a), (d), and (e); and (2) using, carrying, or brandishing a firearm during and in relation to a crime of violence, in violation of § 924(c)(1)(A). Chatrie was arraigned on October 1, 2019,

[9] According to Google's records, Chatrie created a Google account on August 20, 2017. He later opted in to Location History from a Samsung smartphone on July 9, 2018.

and pleaded not guilty. He then moved to suppress the evidence obtained using the geofence warrant.

On March 3, 2022, the district court denied Chatrie's motion to suppress. Although the court voiced concern about the threat geofence warrants pose to user privacy, it declined to resolve whether the geofence evidence was obtained in violation of the Fourth Amendment. Rather, 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, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).

Chatrie subsequently entered a conditional guilty plea and was sentenced to 141 months' imprisonment and 3 years' supervised release. This timely appeal followed.

II. Discussion

Chatrie asks us to hold that the geofence warrant violated his Fourth Amendment rights and that the fruits of the warrant should be suppressed. He argues that the government conducted a Fourth Amendment search because it invaded his reasonable expectation of privacy in his location information. He further claims that the geofence warrant authorizing the search was invalid for lack of probable cause and particularity. Finally, he asserts that the good-faith exception to the exclusionary rule does not apply to this warrant.

The district court denied Chatrie's motion to suppress based on the good-faith exception. I agree that the motion should have been denied, but for an antecedent reason: Chatrie did not have a reasonable expectation of

privacy in two hours' worth of Location History data voluntarily exposed to Google. So the government did not conduct a search when it obtained this information from Google, and so no warrant was required at all. The district court should be affirmed on that straightforward basis. *See United States v. Smith*, 395 F.3d 516, 519 (4th Cir. 2005) (holding that we may affirm a district court "on any grounds apparent from the record").

A. *Carpenter*, *Beautiful Struggle*, and the Third-Party Doctrine

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. To trigger its protections, the government must conduct a "search" (or "seizure") covered by the Fourth Amendment. That's the first step in a Fourth Amendment search analysis, and this case should not get past it.

"For much of our history, Fourth Amendment search doctrine was 'tied to common-law trespass' and focused on whether the government 'obtains information by physically intruding on a constitutionally protected area.'" *Carpenter v. United States*, 585 U.S. 296, 304, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018) (quoting *United States v. Jones*, 565 U.S. 400, 405, 406 n.3, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012)). This trespass-based approach remains alive and well to this day. *See*, *e.g.*, *Jones*, 565 U.S. at 405–08, 132 S.Ct. 945.

But as American society changed and technology developed, so too did the government's ability to intrude

on sensitive areas. *Carpenter*, 585 U.S. at 305, 138 S.Ct. 2206; *see generally* Orin Kerr, *The Digital Fourth Amendment* (2025). So the Supreme Court birthed a new privacy-based framework in *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). Under *Katz*, a search occurs when the government invades an individual's reasonable expectation of privacy. *Id.* at 351, 88 S.Ct. 507; *id.* at 360, 88 S.Ct. 507 (Harlan, J., concurring); *see also Smith v. Maryland*, 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). This privacy-based approach augments the prior, trespass-based approach by providing another way to identify a Fourth Amendment search. *See Jones*, 565 U.S. at 405–08, 132 S.Ct. 945; *Carpenter*, 585 U.S. at 304, 138 S.Ct. 2206.

Though sweeping, *Katz*'s reasonable-expectation framework is not boundless. One important limit on its scope is the "third-party doctrine." The Supreme Court has long recognized that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743–44, 99 S.Ct. 2577. This is because he "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *United States v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). And it holds true "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* Thus, in *Miller*, the Court held that the government did not conduct a search when it obtained an individual's bank records from his bank, since he voluntarily exposed those records to the bank in the ordinary course of business. *Id.* at 443, 96 S.Ct. 1619. Likewise, in *Smith*,

the Court held that the government did not conduct a search when it used a pen register to record outgoing phone numbers dialed from a person's telephone, because he voluntarily conveyed those numbers to his phone company when placing calls. 442 U.S. at 742, 99 S.Ct. 2577.[10]

Despite its clear mandate, the third-party doctrine has proved difficult to implement in the digital age. After all, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417, 132 S.Ct. 945 (Sotomayor, J., concurring). If they lack Fourth Amendment protections for any electronically shared data, then the government could access whole swaths of private information free from constitutional scrutiny.

The Supreme Court addressed this tension in a series of cases involving the government's use of location-tracking technology. First, in *United States v. Knotts*, the Court held that the government did not conduct a search when it placed a tracking device in a container purchased by one of Knotts's coconspirators and used it to monitor his short trip to Knott's cabin. 460 U.S. 276, 278–80, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983). The Court explained that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of

---

[10] Of course, *Miller* and *Smith* were not the only cases to invoke this principle. The Court has applied the third-party doctrine to other kinds of information, too, including incriminating conversations with undercover agents, *United States v. White*, 401 U.S. 745, 749–52, 91 S.Ct. 1122, 28 L.Ed.2d 453 (1971), and tax documents given to an accountant, *Couch v. United States*, 409 U.S. 322, 335, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973).

privacy in his movements from one place to another," since he "voluntarily convey[s] [them] to anyone who want[s] to look." *Id.* at 281, 103 S.Ct. 1081. The use of the tracker merely "augment[ed]" existing police capabilities and "amounted principally to the following of an automobile on public streets and highways." *Id.* at 281–82, 103 S.Ct. 1081. Yet the Court reserved whether it would treat long-term surveillance differently. *Id.* at 283–84, 103 S.Ct. 1081.[11]

---

[11] Separately, the Court held that police did not conduct a search when they observed the beeper on the premises of Knotts's cabin. *Knotts*, 460 U.S. at 284–85, 103 S.Ct. 1081. "[T]here is no indication," the Court explained, "that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin." *Id.* at 285, 103 S.Ct. 1081. So the government did not invade Knott's reasonable expectation of privacy in his home when it observed the beeper on his property.

Yet the Court reached the opposite result one year later in *United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984). *Karo*, like *Knotts*, involved police use of a beeper to monitor the movement of a container; only this time, officers used it to determine whether the container remained inside a home rented by several of the defendants. *Id.* at 709–10, 104 S.Ct. 3296. The Court held that this use of the beeper "violate[d] the Fourth Amendment rights of those who ha[d] a justifiable interest in the privacy of the residence." *Id.* at 714, 104 S.Ct. 3296. The beeper allowed the government to obtain information that it otherwise could not have obtained—that the item was still inside the house—without entering the home itself, which would have required a warrant. *Id.* at 715, 104 S.Ct. 3296. It therefore intruded on the reasonable expectation of privacy of all who had a Fourth Amendment interest in that home. *Id.* at 719, 104 S.Ct. 3296 (ruling that the evidence was inadmissible against "those with privacy interests in the house"); *see also Kyllo v. United States*, 533 U.S. 27, 40, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) ("Where, as here, the Government uses a device

This issue later resurfaced in *Jones*. There, the government attached a GPS device to Jones's automobile and used it to track his movements for twenty-eight days. *Jones*, 565 U.S. at 402–04, 132 S.Ct. 945. Applying the original property-based approach, the Court decided that the government's physical trespass on Jones's vehicle amounted to a search. *Id.* at 404–05, 132 S.Ct. 945. But in separate opinions, five Justices would have held that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"—even though a person's movements are seemingly shared with third parties. *Id.* at 430, 132 S.Ct. 945 (Alito, J., concurring in the judgment); *id.* at 415, 132 S.Ct. 945 (opinion of Sotomayor, J.). Such long-term monitoring violates reasonable expectations of privacy because "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 430, 132 S.Ct. 945 (opinion of Alito, J.).

After *Jones*, it was unclear how the Court would decide a case involving long-term monitoring without a physical trespass. The Court eventually considered this issue in *Carpenter*. *Carpenter* involved government access to

---

that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."). *But see Karo*, 468 U.S. at 716 n.4, 104 S.Ct. 3296 (distinguishing *Rawlings v. Kentucky*, 448 U.S. 98, 100 S.Ct. 2556, 65 L.Ed.2d 633 (1980), since the defendant in that case did not have a reasonable expectation of privacy in the place searched).

historical cell-site location information ("CSLI")—a time-stamped record that is automatically generated every time any cell phone connects to a cell site. 585 U.S. at 300–01, 138 S.Ct. 2206. The government requested—without a warrant—7 days' worth of Carpenter's historical CSLI from one wireless carrier and 152 days' worth from another. *Id.* at 302, 138 S.Ct. 2206.[12] It then used this information to tie him to the scene of several robberies. *Id.* Carpenter moved to suppress the evidence, arguing that the government had conducted a search without the necessary warrant. *Id.*

The Court began by noting that government access to CSLI "does not fit neatly under existing precedents" but "lie[s] at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake." *Id.* at 306, 138 S.Ct. 2206. Starting with the location-tracking cases, the Court found that CSLI "partakes of many of the qualities of"—and in some ways, exceeds—"the GPS monitoring we considered in *Jones*." *Id.* at 309–13, 138 S.Ct. 2206. The unprecedented surveillance capabilities afforded by CSLI, retrospective over days, reveal—directly and by deduction—a broad array of private information. *Id.* at 310–12, 138 S.Ct. 2206. The Court thus explained that CSLI provides law enforcement "an all-encompassing record of the holder's whereabouts" over that period, *id.* at 311, 138 S.Ct. 2206, allowing it to peer into a person's "privacies of life," including "familial, political,

---

[12] Although the government requested 7 days' worth of CSLI from one wireless carrier and 152 days' worth from the other, it received only 2 days' worth from the former and 127 days' worth from the latter. *Carpenter*, 585 U.S. at 302, 138 S.Ct. 2206.

professional, religious, and sexual associations." *Id.* (first quoting *Riley v. California*, 573 U.S. 373, 403, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014); and then quoting *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (opinion of Sotomayor, J.)). Such access—at least, to seven days' worth of CSLI—invades the reasonable expectation of privacy individuals have "in the whole of their physical movements." *Id.* at 310 & n.3, 138 S.Ct. 2206.

That Carpenter "shared" his CSLI with his wireless carriers didn't change the Court's conclusion. *Id.* at 314, 138 S.Ct. 2206. Rejecting the government's invocation of the third-party doctrine, the Court found that the rationales that historically supported the doctrine did not apply to the facts at issue. *Id.* It first considered "'the nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'" *Id.* (quoting *Miller*, 425 U.S. at 442, 96 S.Ct. 1619). And it found that, unlike the bank records in *Miller* or the pen register in *Smith*, CSLI is extremely revealing of a person's private life. *Id.* at 314–15, 138 S.Ct. 2206 (noting that CSLI is a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years"). The government's access of such a large quantity of detailed information therefore "implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Id.* at 315, 138 S.Ct. 2206.

The Court then found that Carpenter did not *voluntarily* expose this "comprehensive dossier of his physical movements" to his wireless carriers. *Id.* Rather, "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the

user beyond powering up." *Id.* Put differently, having and operating a cell phone automatically and necessarily requires the transmission of one's CSLI to the wireless carrier. And cell phones "are 'such a pervasive and insistent part of daily life,'" the Court explained, "that carrying one is indispensable to participation in modern society." *Id.* (quoting *Riley*, 573 U.S. at 385, 134 S.Ct. 2473). So "in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over" this information. *Id.* (second alteration in original) (quoting *Smith*, 442 U.S. at 745, 99 S.Ct. 2577). The Court thus declined to extend the third-party doctrine to overcome Carpenter's Fourth Amendment protection. *Id.*

The Court emphasized that its holding was "a narrow one." *Id.* at 316, 138 S.Ct. 2206. It did not decide how the Fourth Amendment applies to other forms of data collection, like real-time (as opposed to historical) CSLI or "tower dumps" (*i.e.*, records of phones connected to a particular cell tower over a given period). *Id.* Nor did it jettison the third-party doctrine's application in other contexts. *Id.* All it held was that the government's acquisition of at least seven days' worth of historical CSLI is a search within the meaning of the Fourth Amendment. *Id.* at 316, 310 n.3, 138 S.Ct. 2206.

Three years later, we clarified the scope of *Carpenter*'s holding in *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021) (en banc). *Beautiful Struggle* involved a Fourth Amendment challenge to the City of Baltimore's aerial-surveillance program. *Id.* at 333. The program captured aerial photos of thirty-two square city miles every second for "at least 40 hours a week, obtaining an estimated twelve hours of coverage

of around 90% of the city each day." *Id.* at 334. We interpreted *Carpenter* to "solidif[y] 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 (second alteration in original) (quoting *Carpenter*, 585 U.S. at 310, 138 S.Ct. 2206). And we held that Baltimore's program crossed that line because it afforded the government retroactive access to a "detailed, encyclopedic" record of every person's movement in the city across days and weeks. *Id.* (quoting *Carpenter*, 585 U.S. at 309, 138 S.Ct. 2206). The sheer breadth of this information "enable[d] deductions about 'what a person does repeatedly, what he does not do, and what he does ensemble,' which 'reveal[s] more about a person than does any individual trip viewed in isolation.'" *Id.* at 342 (second alteration in original) (quoting *United States v. Maynard*, 615 F.3d 544, 562–63 (D.C. Cir. 2010)). So we held that, when it accessed this information, the government intruded on reasonable expectations of privacy and thereby conducted a search. *Id.* at 346.[13]

B. Application

Relying on *Carpenter*, Chatrie argues that the government conducted a search when it obtained his Location History data from Google. [14] I disagree.

---

[13] The government did not invoke the third-party doctrine in *Beautiful Struggle*.

[14] Chatrie does not argue that the government conducted a search when it obtained his subscriber information from Google at Step Three of the geofence warrant process. This is probably because we

Carpenter identified two rationales that justify applying the third-party doctrine: the limited degree to which the information sought implicates privacy concerns and the voluntary exposure of that information to third parties. Both rationales apply here.[15] Because Chatrie did not have a reasonable expectation of privacy in the two hours' worth of Location History data that law enforcement obtained from Google at Step Two, I would find that the government did not conduct a search by obtaining his information at Steps One or Two.[16]

Start with the nature of the information sought. *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206. At Step Two, the government requested and obtained only two hours' worth of Chatrie's Location History data.[17] By no means

---

have already held that individuals do not have a reasonable expectation of privacy in subscriber information they provide to an internet provider. *See United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010).

[15] Because both rationales apply here, I need not decide whether the voluntary disclosure of more expansive data would take a case outside the third-party doctrine. *See Carpenter*, 585 U.S. at 314–15, 138 S.Ct. 2206 (holding that the third-party doctrine did not apply to the involuntary disclosure of expansive data).

[16] By focusing our inquiry at Step Two, we consider the broadest set of information about Chatrie that was provided to the government. At Step Two the government obtained more information about Chatrie than at Step One. But because the two hours of data the police accessed at Step Two did not reveal a "detailed, encyclopedic" chronicle of Chatrie's life, the smaller dataset accessed at Step One didn't either.

[17] Chatrie suggests that we overlook the relevant dataset: *All* the data in Sensorvault that Google trawled to find the narrower set of information it gave the police. This argument relies on the premise that *Google* performed a Fourth Amendment search just by digging

was this an "all-encompassing record of [Chatrie's] whereabouts ... provid[ing] an intimate window into [his] person[al] life." *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206. All the government had was an "individual trip viewed in isolation," which, standing alone, was not enough to "enable[ ] deductions about 'what [Chatrie] does repeatedly, what he does not do, and what he does ensemble.'"[18] *Beautiful Struggle*, 2 F.4th at 342 (quoting

---

through its own data, most of which it never turned over. But precedent squarely forecloses this argument. *See Beautiful Struggle*, 4 F.4th at 344 ("*Carpenter* was clear on that issue: a search took place 'when the *Government accessed CSLI* from the wireless carriers.'" (quoting *Carpenter*, 585 U.S. at 313, 138 S.Ct. 2206) (emphasis added)). Whether we focus on Step One or Step Two, the right question is what information Google gave to the *government*, not what data Google perused to find that information.

This mistake of considering the Fourth Amendment search to be Google's efforts to locate information in its database does appear to have animated the Fifth Circuit's decision in *United States v. Smith*, 110 F.4th 817, 836–38 (5th Cir. 2024). *Cf.* Orin Kerr, *The Fifth Circuit Shuts Down Geofence Warrants—And Maybe a Lot More*, The Volokh Conspiracy (Aug. 13, 2023) (finding *Smith*'s general-warrant-by-Google theory "not just wrong, but basically bananas").

[18] Chatrie raises the possibility that a geofence warrant could reveal a person's movements within a constitutionally protected space, like his home. *See Karo*, 468 U.S. at 716–17, 104 S.Ct. 3296; *Kyllo*, 533 U.S. at 40, 121 S.Ct. 2038. The district court expressed similar concerns and noted that the instant geofence warrant included potentially sensitive locations within its radius. But this is an issue for future cases, not the one before us. Chatrie does not contend that the warrant revealed his own movements within his own constitutionally protected space. And to the extent that it might have captured his or others' movements in another person's protected space, Chatrie lacks standing to assert their potential Fourth Amendment claims. *See Rakas v. Illinois*, 439 U.S. 128, 133–

Maynard, 615 F.3d at 562–63). The information obtained was therefore far less revealing than that obtained in *Jones*, *Carpenter*, or *Beautiful Struggle* and more like the short-term public movements in *Knotts*, which the Court found were "voluntarily conveyed to anyone who wanted to look." *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206 (quoting *Knotts*, 460 U.S. at 281, 103 S.Ct. 1081).[19] A record of a person's single, brief trip is no more revealing than his bank records or telephone call logs. *See Miller*, 425 U.S. at 442, 96 S.Ct. 1619; *Smith*, 442 U.S. at 742, 99 S.Ct. 2577. Chatrie thus did not have a "legitimate 'expectation of privacy,'" in the information obtained by the government, so the first rationale for the third-party doctrine applies here. *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206 (quoting *Miller*, 425 U.S. at 442, 96 S.Ct. 1619).

Furthermore, Chatrie voluntarily exposed his location information to Google by opting in to Location History. *Id.* at 315, 138 S.Ct. 2206. Consider again how Location History works. Location History is an optional setting that adds extra features, like traffic updates and targeted advertisements, to a user's experience. But it is "off by default" and must be affirmatively activated by

---

34, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978); *Brown v. United States*, 411 U.S. 223, 230, 93 S.Ct. 1565, 36 L.Ed.2d 208 (1973).

[19] Chatrie argues that the amount of information obtained shouldn't matter, given the accuracy with which Location History can estimate a user's location. Yet the question is not whether the government knew with exact precision what Chatrie did on an "individual trip viewed in isolation," *Beautiful Struggle*, 2 F.4th at 342 (quoting *Maynard*, 615 F.3d at 562), but whether it gathered enough information from many trips to "reveal intimate details through habits and patterns," *id.* at 341. That was not the case here.

a user before Google begins tracking and storing his location data. J.A. 1333–34. Of course, once Google secures this consent, it monitors his location at all times and across all devices. Yet even then, Google still affords the user ultimate control over how his data is used: If he changes his mind, he can review, edit, or delete the collected information and stop Google from collecting more. Whether Google tracks a user's location, therefore, is entirely up to the user himself. If Google compiles a record of his whereabouts, it is only because he has authorized Google to do so.

Nor is a user's consent secured in ignorance, either. *See Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206 (explaining that the third-party doctrine applies to information "knowingly shared with another"). To the contrary, the record shows that Google provides users with ample notice about the nature of this setting. Before Google allows a user to enable Location History, it first displays text that explains the basics of the service. The text states that enabling Location History "[s]aves where you go with your devices," meaning "[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences." It also informs a user about his ability to view, delete, or change his location data.[20] A user cannot opt in to Location History without seeing this text.

So unlike with CSLI, a user knowingly and voluntarily exposes his Location History data to Google. First, Location History is not "'such a pervasive and insistent

---

[20] Google provides additional notice of this setting in its Privacy Policy.

part of daily life' that [activating it] is indispensable to participation in modern society." *Carpenter*, 585 U.S. at 315, 138 S.Ct. 2206 (quoting *Riley*, 573 U.S. at 385, 134 S.Ct. 2473). *Carpenter* found that it is impossible to participate in modern life without a cell phone. *Id.* But the same cannot be said of Location History. While Location History offers a few useful features to a user's experience, its activation is unnecessary to use a phone or even to use apps like Google Maps. Chatrie gives us no reason to think that these added features are somehow indispensable to participation in modern society and that his decision to opt in was therefore involuntary. That two-thirds of active Google users have not enabled Location History is strong evidence to the contrary. *Cf. Riley*, 573 U.S. at 385, 134 S.Ct. 2473 (noting that, as of 2014, "a significant majority of American adults" owned smartphones). Thus, a user can decline to use Location History and still participate meaningfully in modern society.

Second, unlike CSLI, Location History data is obtained by a user's affirmative act. *Carpenter* noted that "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." 585 U.S. at 315, 138 S.Ct. 2206. But Location History is *off by default* and can be enabled only by a user's affirmative act. A person need not go off the grid by "disconnecting [his] phone from the network ... to avoid" generating Location History data; instead, he can simply decline to opt in and continue using his phone as before. *See id.* Thus, "in [every] meaningful sense," a user who enables Location History "voluntarily 'assume[s] the risk'" of turning over his location information. *Id.* (quoting *Smith*, 442 U.S. at 745,

99 S.Ct. 2577). So the second rationale for the third-party doctrine applies here, too.

The third-party doctrine therefore squarely governs this case. The government obtained only two hours' worth of Chatrie's location information, which could not reveal the privacies of his life. And Chatrie opted in to Location History on July 9, 2018. This means that he knowingly and voluntarily chose to allow Google to collect and store his location information. In so doing, he "t[ook] the risk, in revealing his affairs to [Google], that the information [would] be conveyed by [Google] to the Government." *Miller*, 425 U.S. at 443, 96 S.Ct. 1619. He cannot now claim to have had a reasonable expectation of privacy in this information. *See Smith*, 442 U.S. at 743–44, 99 S.Ct. 2577. The government therefore did not conduct a search when it obtained the data.[21]

---

[21] Nor has Chatrie shown a property interest in his Location History data. Chatrie does not cite any positive law (state or federal) that gives him an ownership interest in his Location History data. *See Carpenter*, 585 U.S. at 331, 138 S.Ct. 2206 (Kennedy, J., dissenting); *id.* at 353–54, 138 S.Ct. 2206 (Thomas, J., dissenting); *id.* at 402, 138 S.Ct. 2206 (Gorsuch, J., dissenting). Nor does he claim that he could bring a tort suit if this information were stolen. *See id.* at 353, 138 S.Ct. 2206 (Thomas, J., dissenting). Instead, he relies largely on the fact that Google describes Location History as "*your* information," J.A. 39 (emphasis added), and as a user's "virtual journal," J.A. 128. But this is an incredibly thin reed on which to hang such a bold pronouncement. Though we issue no opinion on whether Google can create a property interest merely by saying one exists, Google at least knows how to recognize preexisting property rights when it wants to. At the time Chatrie opted in to Location History, Google explicitly labelled digital cloud content as user property. *See* J.A. 2083 ("You retain ownership of any intellectual property rights that you hold in that content. In

* * *

The Fourth Amendment is an important safeguard to individual liberty. But its protections are not endless. To transgress its command, the government must first conduct a search. I would hold that the government did not conduct a Fourth Amendment search when it accessed two hours' worth of Chatrie's location information that he voluntarily exposed to Google.

---

short, what belongs to you stays yours."). But Google used no such language to describe its location services. *See* J.A. 2051 (describing location information as content Google "collect[s]" and omitting mention of property rights); J.A. 1339–40 (omitting mention of property rights at the initial opt-in). We therefore cannot hold, based on the record before us, that Chatrie had a property interest in his Location History data.

TOBY HEYTENS, Circuit Judge, with whom Judges HARRIS and BERNER join, concurring:

Whether or not there was a Fourth Amendment violation here, I think the district court rightly declined to prescribe the "strong medicine" of excluding otherwise admissible evidence. *United States v. Janis*, 428 U.S. 433, 453, 96 S.Ct. 3021, 49 L.Ed.2d 1046 (1976) (quotation marks removed).

"The fact that a Fourth Amendment violation occurred ... does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009). Exclusion of unlawfully seized evidence is "not a personal constitutional right, nor is it designed to redress the injury occasioned by an unconstitutional search." *Davis v. United States*, 564 U.S. 229, 236, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011) (quotation marks removed). Rather, the exclusionary rule is a "judicially created remedy" whose "sole purpose ... is to deter future Fourth Amendment violations." *United States v. Calandra*, 414 U.S. 338, 348, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974) (first quote); *Davis*, 564 U.S. at 236–37, 131 S.Ct. 2419 (second quote).

"Real deterrent value is a necessary condition for exclusion, but it is not a sufficient one." *Davis*, 564 U.S. at 237, 131 S.Ct. 2419 (quotation marks removed). The Supreme Court's cases "have thus limited" the exclusionary "rule's operation to situations in which [its deterrent] purpose is thought most efficaciously served." *Id.* (quotation marks removed). In particular, "[t]o 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 judicial system" when relevant and reliable evidence is suppressed. *Herring*, 555 U.S. at 144, 129 S.Ct. 695. In contrast, when law enforcement officials "act with an objectively reasonable good-faith belief that their conduct is lawful," "the deterrence rationale loses much of its force, and exclusion cannot pay its way." *Davis*, 564 U.S. at 238, 131 S.Ct. 2419 (quotation marks removed).

In my view, exclusion is unwarranted here for two related reasons.

First, the legal landscape was uncertain when this investigation happened. "Responsible law enforcement officers will take care to learn what is required of them under Fourth Amendment precedent and will conform their conduct to [those] rules." *Davis*, 564 U.S. at 241, 131 S.Ct. 2419 (quotation marks removed). But here there were no clear guideposts to follow. The investigating officer was using "rapidly developing technology" while faced with a "dearth of court precedent." *United States v. McLamb*, 880 F.3d 685, 691 (4th Cir. 2018) (first quote); *United States v. Smith*, 110 F.4th 817, 840 (5th Cir. 2024) (second quote). Indeed, when the officer was investigating this case, it appears no court had examined the validity of (or constitutional restrictions on) geofence warrants.

Second, the officer did what we expect reasonable officers to do when faced with such uncertainty. The officer knew he "had sought three other geofence warrants in the past" that magistrates had approved. JA

1349; see *United States v. Carpenter*, 926 F.3d 313, 318 (6th Cir. 2019) (noting that, at the relevant time, "[t]wo magistrate judges" had issued orders based on the same statute the Supreme Court later held could not constitutionally justify obtaining the defendant's cell-site location information without a warrant). "Before seeking those warrants," the officer "consulted with prosecutors, who approved them." JA 1349; see *McLamb*, 880 F.3d at 691 (noting officers had "consulted with attorneys from the Department of Justice"); *Smith*, 110 F.4th at 839 (officers "had conversations with other law enforcement officers and the U.S. Attorney's Office prior to submitting their warrant"). And here, for the fourth time, the officer sought and obtained a warrant from a judicial officer.

The Supreme Court has said the exclusionary rule should be used to "deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring*, 555 U.S. at 144, 129 S.Ct. 695. Any Fourth Amendment error here did "not rise to that level." *Id.* Indeed, "one can understand" why a reasonable officer "might have believed" he had done all the Fourth Amendment required. *Carpenter*, 926 F.3d at 318; see *United States v. Katzin*, 769 F.3d 163, 177–87 (3d Cir. 2014) (en banc). And because the investigating officer could have had "an objectively reasonable good-faith belief that [his] conduct [was] lawful," I think the district court was right to withhold "the harsh sanction of exclusion." *Davis*, 564 U.S. at 238, 240, 131 S.Ct. 2419 (quotation marks removed).

BERNER, Circuit Judge, with whom Judges GREGORY, WYNN, THACKER, and BENJAMIN join, and with whom Judge HEYTENS joins as to Parts I, II(A), and II(B), concurring:

Our Fourth Amendment jurisprudence recognizes that the balance between individual privacy and public safety is a delicate one. Technology's threat to that balance lies at the heart of this case. Prohibiting the government from using geofence warrants in all but the rarest of cases would unnecessarily frustrate criminal investigations. At the same time, allowing the government warrantless access to individuals' non-anonymous location data would swing the pendulum too far in the other direction.

In this case, the Government used a geofence warrant to investigate a bank robbery. After early leads failed to generate a suspect, the Government sought information about individuals whose cellphones were near the scene of the crime. A magistrate granted the Government's application for a geofence warrant. Pursuant to this warrant, the Government sent Google three separate, increasingly probing, requests for Google users' Location History data.

In its first request, the Government asked Google to produce a dataset showing pseudonymized [1] Google

[1] Pseudonymization is the process of removing personal identifiers (such as names, email addresses, and phone numbers) from a dataset and replacing them with identifiers (such as random alphanumeric codes) that are not tied to individuals' identities. Pseudonymized data is not necessarily anonymous, however. Through certain clues

users' movements within a 150-meter radius of the bank—the initial "geofence"—during the one-hour period surrounding the robbery. Because of the narrow parameters of this request, the pseudonymized Location History was not likely to be traceable to the identities of particular Google users.

In its second request, the Government sought additional Location History data unconfined by any geographic boundary. Though the Government asked Google to produce a pseudonymized dataset, the broad scope of the request meant that the Government would likely be able to associate that Location History data with the identities of specific people. The data would, for example, likely show pseudonymized Google users entering particular homes and offices. Thus, it was not truly anonymous.

Finally, in its third request, the Government expressly asked Google to reveal the names, email addresses, and phone numbers associated with certain pseudonymized Google users identified in the second dataset. One of those users was Okello Chatrie.

The Government's requests raise two Fourth Amendment questions: (1) whether Chatrie held a reasonable expectation of privacy in his Location History data, and (2) if so, whether the warrant the Government used to acquire this data was supported by probable cause.

---

or pieces of information, it may be possible to unmask the personal identities of individuals contained in a pseudonymized dataset.

Unlike our colleagues on the Fifth Circuit, I do not believe that geofence warrants are categorically unconstitutional. *See United States v. Smith*, 110 F.4th 817, 838 (5th Cir. 2024). Individuals lack a reasonable expectation of privacy in Location History data that is truly anonymous, meaning that—as evaluated at the time of the government's request—the data is not likely to be traceable to specific individuals. An individual does not have a reasonable expectation of privacy in the mere fact that a certain number of unknown individuals were located near a public place at a particular time, even if he happened to be one of those individuals. I would thus hold that Government's first request to Google did not result in a Fourth Amendment search. Because of the (1) short duration of the request, (2) limited size of the geofenced area, and (3) public nature of the geofenced area, the Location History data that the Government initially requested from Google was not likely to be traceable to any specific individual, including Chatrie. Consequently, the initial request did not infringe upon Chatrie's reasonable expectation of privacy.

Under the framework established by the Supreme Court in *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018), however, I would hold that individuals do have a reasonable expectation of privacy in their *non-anonymous* Location History data. This includes pseudonymized data that, based on the parameters of a particular request, is likely to be traceable to the identities of specific individuals. The Government thus conducted a Fourth Amendment search when it acquired Chatrie's non-anonymous Location History data through its second and third requests to Google.

Before conducting a Fourth Amendment search, law enforcement "must generally obtain a warrant supported by probable cause." *Carpenter*, 585 U.S. at 316, 138 S.Ct. 2206. Because the Government lacked probable cause to search any specific Google user at the time it applied for the geofence warrant, this warrant was invalid and the Government's search of Chatrie violated the Fourth Amendment.

I. Background

On the afternoon of May 20, 2019, an unknown individual robbed a bank in Virginia. The robber pointed a gun at the bank manager and stole approximately $195,000. He then fled the scene before police could respond, and law enforcement was unable to find him through witness accounts, tips, and security footage.

In reviewing the bank's security footage, however, a detective noticed that the robber appeared to have been holding a cellphone when he walked into the bank. Knowing that Google possesses location data on millions of cellphones, the detective applied for and obtained a warrant seeking information from Google about all cellphones within a certain radius of the bank—a perimeter known as a geofence—around the time of the crime. Google complied with the geofence warrant. Through three separate requests to Google, the Government ultimately obtained geolocation data that enabled it to identify Chatrie as the suspect. This appeal concerns Chatrie's motion to suppress that data.

Google had been keeping a record of Chatrie's movements through its Location History tool. Location

History automatically records the location of a cellphone, even when the user is not actively using his phone or receiving incoming messages. To obtain a phone's latitude and longitude coordinates, Location History draws from GPS information, Bluetooth, cellular towers, IP address information, and the signal strength of nearby Wi-Fi networks. All data collected by Location History is stored in a Google-controlled repository known as "Sensorvault." Though individuals can decline to enable Location History, Google repeatedly prompts users to enable the feature when they open certain mobile apps.

Location History logs comprehensive and precise data from cellphones that enable location tracking. Location History records a phone's location approximately every two minutes. In certain circumstances, Google can estimate a phone's location down to three meters. Location History even allows Google to estimate a phone's elevation, with precision that can potentially infer the specific floor of an apartment building where a user is located. To show a phone's location, Location History displays a point on a map and depicts around that point a radius known as a "confidence interval." The smaller the radius around a phone's estimated location, the more confident Google is in that phone's exact location. A phone is somewhere inside the given confidence interval over two-thirds of the time.

Several years ago, Google worked with law enforcement to develop a three-step process for responding to geofence warrants. Each "step" begins with a new request from law enforcement to Google. The Government in this case followed Google's three-step

process. It is worth emphasizing that Google's three-step process was neither designed nor mandated by a magistrate. The process merely expresses the preferences and policy of Google, a private company.

The Government submitted a warrant application that outlined the broad contours of Google's three-step process. Under this process, the second and third requests are necessarily formulated based on Google's responses to the preceding requests. Consequently, at the time the Government applied for the geofence warrant, it could not have explained the specific rationale that would ultimately support its second and third requests.

At step one, the Government requested pseudonymized data showing all Google users' movements within a 150-meter radius of the bank during the one-hour period surrounding the robbery. The geofence perimeter primarily encompassed public streets. In response to the Government's first request, Google produced a pseudonymized dataset that consisted of 210 discrete location datapoints across 19 unique phones, meaning that the Government obtained numerous datapoints from some of those phones.

After reviewing the data that Google provided in response to the first request, the Government next requested from Google additional Location History data on some of the users identified within the initial geofence. In its second request, the Government asked Google to produce two hours of full Location History data—both inside and outside of the 150-meter

geofence—generated by nine of the 19 Google users identified pseudonymously at step one.

After analyzing the additional Location History data that Google produced in response to the second request, the Government submitted its third and final request. In this request, the Government asked Google to disclose identifying information—names, email addresses, and phone numbers—associated with three of the nine pseudonymous account holders whose data the Government obtained at step two. Google's response revealed that one of the three cellphones belonged to Chatrie. The Government ultimately concluded that Chatrie was the individual responsible for the robbery.

II. Analysis

A. The Third-Party Doctrine and *Carpenter*

The government conducts a Fourth Amendment search when it invades an individual's "reasonable" expectation of privacy. *See Katz v. United States*, 389 U.S. 347, 360–62, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring). Courts often refer to this rule as the "*Katz* test." *E.g., Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). Before conducting a Fourth Amendment search, the government "must generally obtain a warrant supported by probable cause" particular to the persons or things to be searched. *Carpenter*, 585 U.S. at 316, 138 S.Ct. 2206. Chatrie argues that the Government violated his Fourth Amendment rights when it obtained his Location History data without a valid warrant. Chatrie cannot rely on the Fourth Amendment's protections unless he

held a reasonable expectation of privacy in that Location History data.[2]

The *Katz* test applies to all searches and seizures. For a subset of cases within this Fourth Amendment framework, however, additional principles guide courts in evaluating whether an expectation of privacy is "reasonable." "No single rubric definitively resolves which expectations of privacy" are reasonable. *Carpenter*, 585 U.S. at 304, 138 S.Ct. 2206. "[T]he analysis is informed by historical understandings of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." *Id.* at 304–05, 138 S.Ct. 2206 (internal quotation marks and citation omitted).

Where an individual challenges the government's acquisition of his data from a third party, courts have traditionally evaluated reasonableness through the "third-party doctrine," a framework developed across two Supreme Court cases in the 1970s. Those cases, *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), and *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), drew "a line between what a person keeps to himself and what he shares with others." *Carpenter*, 585 U.S. at 307–08, 138 S.Ct. 2206. In describing *Miller* and *Smith*, the *Carpenter* Court explained, "[w]e have previously held

---

[2] Courts often refer to this principle as "Fourth Amendment standing," but it is not a jurisdictional requirement and need not be addressed before considering other aspects of a claim. *Byrd v. United States*, 584 U.S. 395, 410–11, 138 S.Ct. 1518, 200 L.Ed.2d 805 (2018).

that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.' That remains true 'even if the information is revealed on the assumption that it will be used only for a limited purpose.'" *Id.* at 308, 138 S.Ct. 2206 (quoting *Smith*, 442 U.S. at 743–44, 99 S.Ct. 2577 (first quote); *Miller*, 425 U.S. at 443, 96 S.Ct. 1619 (second quote) (internal citations omitted)). Under this doctrine, "the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections." *Id.*

In *Miller*, the Court rejected the assertion that an individual holds a reasonable expectation of privacy in his bank records. The Court explained that these documents were "business records of the banks" that were "exposed to [bank] employees in the ordinary course of business." 425 U.S. at 440, 96 S.Ct. 1619 (first quote), 442, 96 S.Ct. 1619 (second quote). In the Court's view, these were "not confidential communications but negotiable instruments to be used in commercial transactions." *Id.* at 442, 96 S.Ct. 1619.

Three years later, the Court in *Smith* held that an individual lacks a reasonable expectation of privacy in the phone numbers he dials. The Court concluded that the government's use of a pen register, a device that records the outgoing phone numbers dialed on a landline telephone, was not a Fourth Amendment search. 442 U.S. at 745–46, 99 S.Ct. 2577. Because the pen register had "limited capabilities," the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial." *Id.* at 742, 99 S.Ct. 2577. According to the Court, telephone subscribers

knew that the numbers they dialed were used by the telephone company "for a variety of legitimate business purposes," including routing calls. *Id.* at 743, 99 S.Ct. 2577.

In *Carpenter*, the Court confronted the applicability of the third-party doctrine to modern data collection. *Carpenter*, like this case, involved an attempt to identify a robbery suspect. *See* 585 U.S. at 301–02, 138 S.Ct. 2206. After police arrested several men suspected of robbing electronics stores, one of the men gave the government the cellphone numbers of his purported accomplices. *Id.* One of those numbers belonged to Carpenter. *Id.*

The government sought Carpenter's historical cellphone location data. *Id.* at 301–2, 138 S.Ct. 2206. It requested from telecommunications carriers a form of data known as cell-site location information (CSLI). *Id.* at 301, 138 S.Ct. 2206. Cell sites, the sets of radio antennas through which cellphones obtain signals, collect time-stamped records each time a phone taps into a network. *Id.* at 302, 138 S.Ct. 2206. These CSLI records are generated by "[v]irtually any activity on the phone ... including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates." *Id.* at 315, 138 S.Ct. 2206.

Though CSLI can be anonymized, the CSLI provided to law enforcement is not typically anonymous. It reveals the phone number of each device that connects to a particular cell site. A cell site is typically mounted to a tower or pole. *Id.* at 300, 138 S.Ct. 2206. Because cellphones generally connect to the closest cell site, it is

possible to determine a phone's approximate location at any moment by knowing the cell site to which the phone was connected. *See id.* "The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area." *Id.* at 301, 138 S.Ct. 2206. CSLI does not distinguish between the locations of the various devices connected to a particular cell site. It shows only that a device was within a given cell site's coverage area.

The government obtained Carpenter's CSLI through court orders, which are subject to a lower standard of proof than search warrants. *See id.* To obtain a court order, the government merely needs to put forth "specific and articulable facts showing that there are *reasonable grounds to believe*" that the records sought are "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (emphasis added). A search warrant, in contrast, must be supported by "the substantially higher probable cause standard." *United States v. Graham*, 796 F.3d 332, 344 (4th Cir. 2015), *rev'd on other grounds*, 824 F.3d 421 (4th Cir. 2016) (en banc).

The court orders at issue in *Carpenter* requested CSLI generated over a lengthy period of time. The first order sought 152 days of CSLI from one cellphone carrier, which responded by producing records spanning 127 days. 585 U.S. at 302, 138 S.Ct. 2206. The second order requested seven days of CSLI from another carrier, which produced two days of records. *Id.* Carpenter moved to suppress the CSLI data obtained through each of these court orders, arguing that the government violated the Fourth Amendment by acquiring these

records without search warrants. *Id.* at 302, 138 S.Ct. 2206. The government asserted that under the third-party doctrine, Carpenter could not claim a legitimate expectation of privacy in CSLI he knowingly disclosed to his cellphone carriers. *See id.* at 313, 138 S.Ct. 2206.

The *Carpenter* Court rejected the government's invocation of the third-party doctrine. It stated that "there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller*," the cases that form the core of the third-party doctrine, "and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id.* at 314, 138 S.Ct. 2206. In light of this distinction, the Court concluded that "the Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct *category of information*." *Id.* (emphasis added).

The *Carpenter* Court explained that whether one holds a reasonable expectation of privacy in data given to a third party depends on: (1) how revealing that data is, and (2) whether the information was, in practical terms, given to the third party voluntarily. *See id.* at 314–15, 138 S.Ct. 2206. After evaluating both factors, the Court concluded that Carpenter held a reasonable expectation of privacy in the CSLI obtained by the government. *See id.* at 313, 138 S.Ct. 2206.

B. *Carpenter*'s Application to this Case

Applying *Carpenter*'s two factors to this case, I would hold that law enforcement conducts a search when it obtains any amount of an individual's Location History

data that is non-anonymous. This includes Chatrie's Location History data that the Government obtained through its second and third[3] requests to Google. These

---

[3] In asserting that the Government violated his Fourth Amendment rights, Chatrie analyzes the alleged search as a single endeavor, not in discrete steps. Unlike Judge Richardson, however, I do not believe Chatrie forfeited any argument that step three was a Fourth Amendment search. *See* opinion of RICHARDSON, J., at 79 n.14. The Government's request at step three is distinct from the request for subscriber information at issue in *United States v. Bynum*, 604 F.3d 161, 162–64 (4th Cir. 2010). In *Bynum*, a pre-*Carpenter* case, this court held that a Fourth Amendment search did not occur where law enforcement used a subpoena to obtain a Yahoo subscriber's name and physical address. *See id.* at 164. Law enforcement in *Bynum* requested subscriber information associated with a *public-facing* Yahoo screen name—one belonging to a user who had voluntarily posted his photo, location, sex, and age on his Yahoo profile page. *Id.*

Here, in contrast, the Government requested the names, email addresses, and phone numbers associated with *private* numerical identifiers (Device IDs) created internally by Google and associated solely with Google users' Location History data, not with other parts of their Google accounts. These Device IDs were not publicized by or even known to individual Google users. The Government was able to learn of these Device IDs only through responses to its requests for Location History data.

Once the government has obtained a user's pseudonymized Location History data, a request that Google reveal that user's identity is no less a search than had the process been reversed—i.e., had the Government provided Google with a name and email address and asked for two hours of that user's Location History data. That an individual lacks a reasonable expectation of privacy in the answer to the question at issue in *Bynum*—essentially, who is johndoe@yahoo.com?—sheds no light on whether he lacks a reasonable expectation of privacy in the answer to the entirely distinct question at issue here—who is the person that traveled in

requests sought highly revealing data, and the record does not establish whether the disclosure of this information was definitively voluntary.

i. Non-Anonymous Location History Data is Highly Revealing

The Government contends that because Chatrie's disclosure of his Location History data to Google was voluntary, he forfeited any expectation of privacy in that data. Yet *Carpenter* explained that voluntariness is merely one of two considerations under the third-party doctrine. "*Smith* and *Miller*, after all, *did not rely solely on the act of sharing*. Instead, they considered '*the nature of the particular documents sought*' to determine whether 'there is a legitimate "expectation of privacy"' concerning their contents.'" *Id.* at 314, 138 S.Ct. 2206 (emphasis added). *Carpenter* described "voluntary exposure" as the "second rationale underlying the third-party doctrine." *Id.* at 315, 138 S.Ct. 2206. Here, as in *Carpenter*, "[i]n mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature" of historical cellphone location data. *Id.*

The revealing nature of Location History data depends on whether it is anonymous. Though anonymous Location History data is not particularly sensitive, non-anonymous Location History data is highly revealing. Because pseudonymized location data may be non-

---

this precise pattern for two hours? The latter, of course, is far more revealing.

anonymous, evaluating the anonymity of a dataset is not always a straightforward inquiry.

Pseudonymized location data is not anonymous when it can be linked to a particular individual. Whether pseudonymized Location History data is likely to be traceable to a specific person—an inquiry that must be conducted at the time of a request, not *post-hoc*—depends on (1) the duration of the request; (2) the size of the search area; and (3) the nature of the search area. The second and third factors are particularly important. Let's take an example. If the government were to look at pseudonymized Location History data generated within a defined section of I-95 between 7:00 am and 9:00 am on a weekday, it is not likely to be able to determine the identities of the individual drivers. If, on the other hand, the search area were unrestricted or included residential neighborhoods, two hours of Location History data during that same time period could reveal that a pseudonymized Google user traveled from a particular home to a particular company's office building. The government could readily determine that individual user's identity by, for instance, looking at property records and running a LinkedIn search.

This court's en banc decision in *Leaders of a Beautiful Struggle v. Baltimore Police Department* recognized that location data without individual identifiers can still pose a threat to privacy. 2 F.4th 330, 341–42 (4th Cir. 2021). In that case, the government contended that an aerial surveillance program did not infringe upon individuals' reasonable expectations of privacy because it showed people only as "a series of anonymous dots traversing a map of Baltimore." *Id.* at 342 (quotation

omitted). This court emphasized, however, that the particular movements of these dots, "analyzed with other available information, will often be enough for law enforcement to deduce the people behind the pixels." *Id.* at 343.

The pseudonymized Location History data obtained through the Government's first request was anonymous. In that request, the Government sought data depicting all Google users' movements within a 150-meter radius, which encompassed primarily public streets and stores, over a one-hour timeframe. Absent some stroke of luck for the Government, it was exceedingly unlikely that Google's response would reveal the identities of the pseudonymized individuals within that geofence perimeter, even if "analyzed with other available information." *Id.* Through its second request to Google, however, the Government obtained two hours of Location History data belonging to nine pseudonymized individuals. That Location History data was not confined to any geographic boundary. At the time of the second request, law enforcement could have predicted that the pseudonymized data would likely be traceable to Chatrie and the other Google users. As a result, it was non-anonymous.

Carpenter compels the conclusion that individuals have a reasonable expectation of privacy in *all* non-anonymous Location History data, regardless of amount. *Carpenter*'s first factor—the revealing nature of the data—directs courts to consider the *type* of data at issue rather than the amount. To be sure, the *Carpenter* Court stated that its holding was "narrow," 585 U.S. at 316, 138 S.Ct. 2206, and, in a footnote, added

that "we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny .... It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." *Id.* at 310 n.3, 138 S.Ct. 2206. I do not read this disclaimer to suggest that the duration of the request played a significant role in the Court's analysis or decision, however. This footnote was in response to the parties' "alternative" suggestion "that the acquisition of CSLI becomes a search only if it extends beyond a limited period." *Id.* The Court's declining to evaluate this alternative theory was not tantamount to an endorsement of it.[4]

In *Carpenter*, the Court repeatedly analyzed what CSLI technology had the *capacity* to reveal, not what it *actually* revealed in the search at issue. The Court stated that "[t]his case is not about using a phone or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, *over several years*." *Id.* at 315, 138 S.Ct. 2206 (emphasis added) (internal

---

[4] The ambiguous wording in footnote three of *Carpenter* may further evidence its relative insignificance. Footnote three states that "[i]t is sufficient for our purposes today to hold that *accessing* seven days of CSLI constitutes a Fourth Amendment search." *Carpenter*, 585 U.S. at 310 n.3, 138 S.Ct. 2206 (emphasis added). Yet the government *accessed* only two days of CSLI from one of the carriers, Sprint, and the Court gave every indication that this alone constituted a search. "When the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy ... Sprint Corporation and its competitors are not your typical witnesses." *Id.* at 313, 138 S.Ct. 2206.

quotation marks omitted). By its own characterization, then, *Carpenter* was "about" what the third party collected—comprehensive data over several years—rather than what the government requested: data over a seven-day stretch. "The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for *years and years*." *Id.* at 313, 138 S.Ct. 2206 (emphasis added). Further, in responding to Justice Kennedy's dissent, the majority stated that Fourth Amendment protection for the "modern-day equivalents of an individual's own 'papers' or 'effects' ... should extend as well to a detailed log of a person's movements *over several years*." *Id.* at 319, 138 S.Ct. 2206 (emphasis added). "At some point, the dissent should recognize that CSLI is an entirely different *species* of business record." *Id.* at 318, 138 S.Ct. 2206 (emphasis added).

Evaluating the type of data rather than the amount intuitively makes sense under the *Katz* test. An individual's expectation regarding whether a third-party storage service such as iCloud will protect his files does not depend on the number of photos or documents stored. A single file may prove more revealing than dozens of others combined; it is impossible to know in advance. That is true of non-anonymous Location History data as well. The government could look through a week of Location History data and learn little sensitive information about a person, or it could look through two hours of data and learn that the person attended a protest and a place of worship. *See* opinion of WYNN, J., at 48. A warrant must be obtained before a search is conducted, but there is no way of knowing the

sensitivity of a dataset before examining its contents. To align with individuals' actual expectations of privacy, Fourth Amendment protections must turn on the *type* of data—here, non-anonymous cellphone Location History data—rather than the amount.

Location History data, like CSLI, is more revealing than any retrospective surveillance method available at the time the Fourth Amendment was adopted. It is a "newfound tracking capacity [that] runs against everyone .... [P]olice need not even know in advance whether they want to follow a particular individual, or when. Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years." *Carpenter*, 585 U.S. at 312, 138 S.Ct. 2206. Whereas past "attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection," Location History data allows the government to "travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers." *Id.* Google retains Location History data indefinitely—even longer than the five-year period that the carriers at issue in *Carpenter* maintained CSLI. *See id.*

Also like CSLI, Location History data can detail a log of a person's movements over several years. Critically, however, non-anonymous Location History data is far more revealing than CSLI. Judge Wynn pointedly explains the differences. *See* opinion of WYNN, J., at 45-46. Location History has the capacity to record a user's location every two minutes, or an average of 720 times per day. CSLI, in contrast, logged Carpenter's location an average of 101 times per day. *Carpenter*, 585 U.S. at

302, 138 S.Ct. 2206. Location History data is thus more "detailed" and "encyclopedic" than CSLI. *Id.* at 309, 138 S.Ct. 2206. It is also far more precise. Whereas CSLI places an individual "within a wedge-shaped sector ranging from one-eighth to four square miles," *id.* at 312, 138 S.Ct. 2206, Location History can pinpoint an individual's location within three meters. Because non-anonymous Location History data is highly revealing, the first *Carpenter* factor weighs in favor of Chatrie.

ii. Chatrie's Disclosure of His Location History Data was not Sufficiently Voluntary to Defeat His Reasonable Expectation of Privacy

Carpenter requires us to balance the revealing nature of non-anonymous Location History data against a second consideration, the voluntariness with which it is disclosed to Google. Whether the disclosure of data to a third party was "voluntary" is not a binary inquiry but a matter of degree. Here, this factor does not tip decisively in favor of either party. Though the Government describes Location History as a voluntary feature that a user must "affirmatively enable," J.A. 1337, the record shows that individuals may enable Location History without meaningfully consenting to data collection, or at least without understanding the implications of the feature.

Google claims that Location History is disabled by default. Yet for those who download certain Google apps—including popular apps such as Google Maps, Google Photos, and Google Assistant—there is no "default" setting. Google repeatedly requires users to

make a choice. Through pop-up permission screens, users are asked either to grant or deny Google permission to track their location.

Users need not intentionally seek to enable Location History. When a user opens Google Maps for the first time, for example, a permission screen prompts the user to "Get the most from Google Maps," and states that "Google needs to periodically store your location to improve route recommendations, search suggestions, and more." J.A. 1485. A button reading "YES I'M IN" is highlighted in blue, while the option to "SKIP" is not. J.A. 1485. When an individual sets up an Android phone, like the phone used by Chatrie, he is directed to use Google Assistant. Upon opening Google Assistant, he is presented with a header instructing him: "Give your new Assistant permission to help you." J.A. 1980. Below that header, a prompt further instructs the user: "The Assistant depends on these settings in order to work correctly. Turn on these settings." J.A. 1980. One of those settings is Location History. After scrolling, the user is given the options of "NO THANKS" or "TURN ON." J.A. 1124. By selecting "TURN ON," the user enables Location History. Here too, the "TURN ON" button is highlighted in blue, while "NO THANKS" is not. J.A. 748–51.

Google stated that approximately two-thirds of its "active users" have declined to enable Location History, but this figure is misleading. One of Google's experts testified that "active Google users" includes anyone with a Google account on any device, including a computer. That would include those who never downloaded a Google app and were thus never presented with the

choice of enabling Location History. Google does not claim that two-thirds of its users, when confronted with a pop-up permission screen, selected "NO THANKS" rather than "TURN ON." Indeed, Google has provided no data about the percentage of users who declined to enable Location History when prompted to do so. Further, the fact that most Google users' settings were different than Chatrie's does not suggest that he intentionally selected his particular settings, or that they intentionally selected theirs.

Even after reviewing all available information about Location History provided by Google, a user would struggle to determine where his Location History data is stored. Google does not explicitly inform users whether Location History data is stored locally on each phone, or whether it is stored on Google's servers and accessible to Google employees. Further, Google's warnings do not indicate how many times a day Location History data will be collected. The third-party doctrine concerns data that one "knowingly share[s]" with a third party. *Carpenter*, 585 U.S. at 298, 138 S.Ct. 2206. If users cannot determine what kind of data is being collected in the first instance, the disclosure of this data cannot be considered "knowing."

Balancing the two *Carpenter* factors, (1) how much the data can reveal, and (2) whether the data was disclosed voluntarily, I would conclude that the Government conducted a Fourth Amendment search when it obtained Chatrie's non-anonymous Location History data through its second and third requests to Google. Accordingly, Chatrie held a reasonable expectation of

privacy in this data, and obtaining it required a valid warrant.

C. The Government's Warrant Application Was Not Supported by Probable Cause

Upon concluding that the acquisition of Chatrie's Location History data was a Fourth Amendment search requiring a warrant, we must evaluate whether the geofence warrant at issue was valid. Under the Fourth Amendment, a warrant "may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011).

The Government's search, as effectuated through its second and third requests to Google, was not supported by probable cause at the time the geofence warrant issued. Probable cause must be evaluated at the time of the warrant application, not in light of subsequent developments. *See Smith v. Munday*, 848 F.3d 248, 253 (4th Cir. 2017). When the detective applied for the geofence warrant, it would have been impossible for him to describe the facts that would ultimately support his decision to conduct a Fourth Amendment search targeting nine particular individuals.

Before the first request to Google, the detective could make a single representation about the Google users he would ultimately search: they would be among those near the crime scene. That information unequivocally falls short of establishing probable cause. A person's mere proximity to suspected criminal activity "does not,

without more, give rise to probable cause to search that person." *Ybarra v. Illinois*, 444 U.S. 85, 91, 100 S.Ct. 338, 62 L.Ed.2d 238 (1979). The government cannot, for example, search every unit in an apartment building because it has probable cause to believe that some unknown part of the building holds evidence of a crime. *See* Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 4.5(b) (6th ed. 2024); *United States v. Clark*, 638 F.3d 89, 95 (2d Cir. 2011); *cf. Maryland v. Garrison*, 480 U.S. 79, 88 n.13, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987). Instead, a warrant can authorize the search of all persons in a particular place only if there is probable cause to believe *every person* in that place was involved in or witnessed the criminal activity. *Id.* Here, of course, there was no evidence that every individual in the vicinity of the bank around the time of the robbery was involved in the crime. Nor was the purpose of the warrant to identify witnesses.

Unlike in *Illinois v. Lidster*, the purpose of the geofence search was to identify suspects. 540 U.S. 419, 124 S.Ct. 885, 157 L.Ed.2d 843 (2004). The Government's reliance on that case is unavailing. In *Lidster*, the Court held that police did not violate the Fourth Amendment when, a week after a hit-and-run, they set up a roadblock to briefly seize all motorists near the location of the accident. 540 U.S. at 421–23, 124 S.Ct. 885. Those stops—executed without individualized suspicion—were constitutional only because they were conducted to identify witnesses, not suspects. *Id.* at 423, 124 S.Ct. 885. The Court described this as an "information-seeking kind of stop," emphasizing that "[t]he stop's primary law enforcement purpose was not to determine whether a vehicle's occupants were committing a crime, but to ask

vehicle occupants, as members of the public, for their help in providing information about a crime in all likelihood committed by others." *Id.* at 423–24, 124 S.Ct. 885. The Court explained that "[t]he police expected the information elicited to help them apprehend[ ] not the vehicle's occupants, but other individuals." *Id.* at 423, 124 S.Ct. 885. In contrast, *Indianapolis v. Edmond*, 531 U.S. 32, 121 S.Ct. 447, 148 L.Ed.2d 333 (2000), established that a search or seizure conducted to "detect evidence of ordinary criminal wrongdoing" rather than to seek information from witnesses is unconstitutional when the government lacks individualized suspicion. *Id.* at 41, 121 S.Ct. 447.

In this case, the Government makes no claim that its "primary law enforcement purpose" was identifying witnesses. The Government had already interviewed witnesses at the time it applied for the Google warrant. The Government states that the purpose of the warrant was to "was to obtain evidence to help identify and convict the robber and any accomplices." Gov't Br. at 31. The warrant application itself focused on the fact that the *robber* "had a cell phone in his right hand and appeared to be speaking with someone on the device" immediately prior to the robbery. J.A. 112. As a result, the Government alleged that "the requested data/information would have been captured by Google during the requested time." J.A. 112. Further, whereas law enforcement in *Lidster* sought "voluntary cooperation" from potential witnesses, cooperation was not voluntary for potential witnesses whose Location History data was disclosed without their knowledge in response to the geofence warrant.

The Government's reliance on *Zurcher v. Stanford Daily* is similarly misplaced. 436 U.S. 547, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978). In *Stanford Daily*, as in this case, the government applied for a search warrant without particular suspects in mind. *Id.* at 550–51, 98 S.Ct. 1970. There, however, the government did not ultimately search any *individual*. Rather, the government searched only the physical office of the Stanford Daily, rifling through its photos and file cabinets. *See id.* at 551–54, 98 S.Ct. 1970. Though, as here, the government in *Stanford Daily* lacked probable cause to search any individual, it did have reason to believe that evidence of a crime would be located in the office of the Stanford Daily. *Id.* at 551, 98 S.Ct. 1970. As a result, the government had probable cause to conduct the *only* search at issue: the search of the Stanford Daily's office.

The critical distinction the Government misses is that here the search infringed on the Fourth Amendment rights of Google *users*, including Chatrie, not Google. Through its second and third requests to Google, the Government searched data belonging to nine individuals whose Location History was stored in Google's databases. The search at issue in *Stanford Daily* is similar only to the Government's first request to Google, as neither of those undertakings violated any individual's reasonable expectation of privacy. The fact that the Government had probable cause to believe that evidence would be found somewhere on Google's servers did not, without more, provide probable cause to search individual Google users' accounts.

Analyzing Google's anonymous data may have given the Government probable cause subsequently to obtain a

warrant for non-anonymous data. Had the detective gone to a magistrate after analyzing the Google data he received in response to the first request, he may have been able to articulate probable cause to search the Location History of particular Google users, including Chatrie. The detective never went back to the magistrate, however. He sought judicial authorization only once—prior to the first request to Google. Because the detective could not explain why he would eventually search the Location History data of certain, then-unknown users in Google's dataset, he failed to show probable cause to conduct the second and third requests. Under the terms of the geofence warrant, Google, not a magistrate, was the sole entity that could confine the scope of the ultimate search. Probable cause determinations cannot be delegated to private entities. *Cf. Birchfield v. North Dakota*, 579 U.S. 438, 469, 136 S.Ct. 2160, 195 L.Ed.2d 560 (2016) ("Search warrants ... ensure that a search is not carried out unless a *neutral magistrate* makes an independent determination that there is probable cause to believe that evidence will be found." (emphasis added)); *United States v. Rubio*, 727 F.2d 786, 794–95 (9th Cir. 1983).

D. Geofence Warrants are not Categorically Unconstitutional

In *United States v. Smith*, the Fifth Circuit held that a geofence warrant can *never* be supported by particularized probable cause. 110 F.4th at 838. The Fifth Circuit concluded that each request pursuant to Google's three-step process, including the request at step one, constitutes a Fourth Amendment search. In

reaching this conclusion, the Fifth Circuit focused on the mechanics of Google's internal compliance processes:

> Step 1 forces the company to search through its entire database to provide a new dataset that is derived from its entire Sensorvault. In other words, [the Government] cannot obtain its requested location data unless Google searches through the entirety of its Sensorvault—all 592 million individual accounts—for all of their locations at a given point in time.

Id. at 837. The Fifth Circuit reasoned that "these geofence warrants fail at Step 1—they allow the Government to rummage through troves of location data from hundreds of millions of Google users." *Id.* at 837–38.

As Judge Richardson correctly points out, the "592 million" number is a red herring. *See* opinion of RICHARDSON, J., at 80 n.17. The government does not search every user in Google's dataset each time it requests Location History data. A search can occur only when *the government* accesses the requested information, not when a company begins looking through its internal database. *See Beautiful Struggle*, 2 F.4th at 344 ("*Carpenter* was clear on that issue: a search took place 'when the Government *accessed* CSLI from the wireless carriers.'" (emphasis in original) (quoting *Carpenter*, 585 U.S. at 313, 138 S.Ct. 2206)). The proper focus of our inquiry is the data the government obtains, not the size of Google's database. Though the Fifth Circuit refers to this proposition as "breathtaking," *Smith*, 110 F.4th at 838 n.12, any other approach would

be nonsensical. The scope of a search does not depend on what a company's compliance officer incidentally encounters—but never discloses to law enforcement—while looking through the company's database to fulfill a particular request. In *Carpenter*, for example, the duration of the search would not have changed had Sprint stored the requested CSLI in a spreadsheet that contained additional days of CSLI data. Because the detective's first request did not amount to a search of any individual in Google's database, the Fourth Amendment did not require the detective to establish probable cause before submitting that request.[5]

If requests for Google's step-one data constitute Fourth Amendment searches of individuals—thus requiring a warrant—such warrants could not be supported by probable cause in most instances. Obtaining a warrant would require probable cause to search all individuals who fall within a particular geofence. The government would thus need to show probable cause that every individual near the scene of a crime was involved in the crime or witnessed it. Because the government is unlikely to be able to make such a showing in most cases,

---

[5] Even if the initial geofence request was not a Fourth Amendment search, the Stored Communications Act may independently require the government to obtain a warrant before requesting Location History data. *See* 18 U.S.C. § 2703. The Act states that the government must obtain a warrant before compelling an Internet service provider to disclose the "contents" of electronic communications, such as the text of an email. *Id.* § 2703(a), (b)(1)(A). At oral argument, the Government conceded that Location History data is likely "content" within the meaning of the Act. *See* Oral Argument at 1:11:40–1:11:52. Because Chatrie waived any statutory claim, however, we need not reach this issue here.

it would ordinarily be prevented from obtaining geofence warrants altogether.

III. Conclusion

Though this case involves advanced technology and difficult legal questions, complexity does not absolve us of our obligation to interpret the Constitution. I see little benefit in postponing these issues until another day. Deciding this case without reaching the Fourth Amendment issues merely perpetuates the constitutional fog that will allow unlawful searches of Location History data to continue to evade consequence through the good-faith exception.

In my view, the government conducts a Fourth Amendment search when it obtains non-anonymous Location History data. This includes pseudonymous data that is likely to be traceable to a particular individual. Therefore, I would find that the Government conducted a search of Chatrie through its second and third requests to Google. Because the Government relied on a warrant that was not supported by probable cause, its search of Chatrie violated the Fourth Amendment.

GREGORY, Circuit Judge, dissenting:

The Fourth Amendment exists to protect "'the privacies of life' against 'arbitrary power,'" *Carpenter v. United States*, 585 U.S. 296, 305, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018) (quoting *Boyd v. United States*, 116 U.S. 616, 630, 6 S.Ct. 524, 29 L.Ed. 746 (1886)), and requires that law enforcement obtain a warrant prior to conducting a search, *id.* at 304, 138 S.Ct. 2206 (citing *Smith v. Maryland*, 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)). In no uncertain terms, it states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

When officers violate these principles, the exclusionary rule, created by the Supreme Court to safeguard against Fourth Amendment violations, generally prohibits use of illegally obtained evidence to prove the defendant's guilt at trial. *United States v. Stephens*, 764 F.3d 327, 335 (4th Cir. 2014) (collecting cases). However, the exclusionary rule is not a "strict-liability regime," *Davis v. United States*, 564 U.S. 229, 240, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011), and only applies where its application will "deter future Fourth Amendment violations," *id.* at 236–37, 131 S.Ct. 2419; *see also Stephens*, 764 F.3d at 335; *Illinois v. Krull*, 480 U.S. 340, 347, 107 S.Ct. 1160, 94 L.Ed.2d 364 (1987). Where an officer reasonably relies on a warrant later determined to lack probable cause, the good faith exception permits admission of the evidence despite the constitutional violation. *United States v. Leon*, 468 U.S. 897, 918–21, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). Whether evidence

should be excluded or admitted following a Fourth Amendment violation requires us to assess if "a reasonably well[-]trained officer would have known that the search was illegal in light of all of the circumstances." *Herring v. United States*, 555 U.S. 135, 145, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009) (internal quotation marks omitted).

To consider these important questions—whether there is a Fourth Amendment violation, and whether the *Leon* good faith exception should apply—requires courts to examine the underlying warrant and the circumstances pertaining to its issuance and execution. That task will sometimes require courts to wade through murky constitutional and doctrinal waters to provide necessary guidance to district courts, attorneys, law enforcement, and citizens alike. But our Court has decided not to do so here, opting instead to sidestep the complex issues presented in this case. The majority of this Court has decided to affirm the district court's opinion, but its reasoning is fractured.

I concur largely in the writings of Judge Wynn and Judge Berner in finding that there was a constitutional violation, as I believe that the geofence warrant at issue glaringly infringed on the Fourth Amendment. However, I write separately to explain why I believe the good faith exception is inapplicable in this case.

I.

Google account users can opt in to location history on their mobile devices, which allows users to keep track of locations they have visited. J.A. 127. At the time of the

offense, Google processed and stored this location history if users shared it via location reporting. J.A. 125, 129–30. Pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, law enforcement can obtain legal process compelling Google to disclose location information, including through geofence warrants. J.A. 124–25. In conjunction with the Department of Justice, Google developed a three-step anonymization and narrowing protocol in response to these geofence requests. J.A. 1344.

In this case, Detective Hylton swore an affidavit for a geofence warrant for Google users' location history. J.A. 107. The warrant, at Step One, authorized a search for anonymized data of Google users with shared location history for a limited time frame (one hour) and a small geographic scope (150-meter radius) where the crime occurred. *See* J.A. 107, 110–11. At Step Two, it authorized a search expanded in both time (one more hour in total) and geographic scope (completely unbounded) and narrowed to a subset of users. J.A. 110–11, 135–36.[1] And at Step Three, the search included non-anonymized, identifying information for a smaller subset. J.A. 111.

Significantly, the warrant did not explain how law enforcement would narrow the list of users at Steps Two

---

[1] Chatrie argues that the data provided at Step Two could be considered non-anonymized, as an expert could identify each of the nine users based on the data provided, such as where they traveled during the expanded location and time. Oral Argument at 1:37:48, *United States v. Okello Chatrie*, (4th Cir. 2025) (No. 22-4489), https://www.ca4.uscourts.gov/OAarchive/mp3/22-4489-20250130.mp3 (henceforth "Oral Argument).

and Three based on the information obtained at Step One. *See* J.A. 110–11. Even now, the government cannot tell us what justified the more intrusive searches at Steps Two and Three, or how or why there was probable cause to search those individuals. *See e.g.*, Oral Argument at 57:17, 1:10:11. Instead, the warrant gave law enforcement broad discretion to request and obtain a seemingly unlimited amount of data associated with devices identified at Step One, checked only by Google.

At Step One, Google provided anonymized data for nineteen devices located within the geofence—which included homes, a hotel, a large church, and a restaurant—thirty minutes before and after the robbery. J.A. 1354, 1357. At Step Two, Detective Hylton ultimately identified nine devices and requested additional location data for those devices expanded for thirty minutes before and thirty minutes after the one-hour window authorized at Step One, and without any geographic limitations. J.A. 1355. This production allowed Detective Hylton to track those devices outside of the confines of the geofence for an hour before and after the crime was committed. At Step Three, Detective Hylton requested, and Google provided identifying information about the accounts associated with three of the devices identified at Step Two. J.A. 1355–56. Consequently, the warrant permitted Detective Hylton to obtain information that the Constitution forbids without probable cause—the detailed movements of anyone with a device identified at Step One—without any additional judiciary oversight. Such lack of additional judiciary oversight was an error by the magistrate.

But that is not enough. As we know from *Leon*, the magistrate's errors alone are insufficient to warrant suppression of evidence obtained pursuant to a deficient warrant. This is because magistrates are "neutral judicial officers" who have "no stake in the outcome of particular criminal prosecutions." *Leon*, 468 U.S. at 917, 104 S.Ct. 3405. As such, excluding evidence because of a magistrate's error would not deter similar misconduct and may even discourage an officer in the future. *Id.* at 920, 104 S.Ct. 3405 (stating that excluding evidence obtained following an officer's objectively reasonable reliance on a search warrant would "in no way affect his future conduct unless it is to make him less willing to do his duty.") (citation and quotation marks omitted).

"Deference to the magistrate, however, is not boundless." *Id.* at 914, 104 S.Ct. 3405. Reliance on the warrant alone is therefore insufficient to protect against exclusion of the recovered evidence. Such is the case where the warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Id.* at 923, 104 S.Ct. 3405. The good faith exception also does not apply where the facts indicate that the investigating officer "could not have harbored an objectively reasonable belief in the existence of probable cause." *Id.* at 926, 104 S.Ct. 3405. As one of my colleagues concluded in assessing the Fourth Amendment violation in this case, *see* Berner, J., concurring at 109–13 the warrant in this case lacked probable cause. As I will now explain further, the evidence in this case should have been excluded, as "it is clear that ... the officer [had] no reasonable grounds for

believing that the warrant was properly issued." *Leon*, 468 U.S. at 922–23, 104 S.Ct. 3405.

To begin, neither the affidavit nor the warrant explained how law enforcement would conduct its review between the various steps of Google's process. J.A. 107, 110–11. Nevertheless, the warrant authorized Detective Hylton to obtain information at Step Three that was of the most personal nature—account-identifying information—for any account associated with a device he identified from Step One without probable cause for each individual's data. But for what amounted to a general warrant, Detective Hylton would not have otherwise received such information.

Additionally, Detective Hylton had unbridled discretion to determine who would be subject to intrusive and expansive searches. For example, at Step Two, Detective Hylton initially requested additional location data for all nineteen users identified at Step One, expanded for thirty minutes before and thirty minutes after the originally requested one hour window, and without any geographic limitations. J.A. 1354–55; *see also* J.A. 98. His email to Google stated that he was requesting the additional data "in an effort to rule out possible co-conspirators," and that nine of the users "may fit the more likely profile of parties involved." J.A. 98. At oral argument, the government contended that it was looking for witnesses as well. *See* Oral Argument at 53:51. Detective Hylton followed up on his email twice on the two following days. J.A. 100, 1059. He then left two voicemails for a Google specialist; the specialist returned his call and recounted the issues in Detective Hylton's email, describing how his request did not follow

the three-step process and explaining the importance of narrowing his request. J.A. 102, 1584–85. The next day, Detective Hylton sent an email narrowing his request to nine users. J.A. 102, 1059, 1584. Google provided Detective Hylton the anonymized, expanded data for nine users. J.A. 1585. As was explained before, the government cannot explain how or why Detective Hylton narrowed in on the particular users. And at no point during this process did Detective Hylton seek judicial intervention, although the warrant did not contain sufficient probable cause and particularity to authorize these additional searches.

Detective Hylton could not have reasonably believed that the liberty authorized by the warrant was constitutional given the lack of specificity the Fourth Amendment explicitly demands.[2] *United States v. Groh*, 540 U.S. 551, 563, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004) (citing *Harlow v. Fitzgerald*, 457 U.S. 800, 818–19, 102 S.Ct. 2727, 73 L.Ed.2d 396 (1982)) ("Given that the particularity requirement is set forth in the test of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid."). On its face, the warrant lacked the requisite constitutional requirements to conduct

---

[2] *See, e.g., Groh v. Ramirez*, 540 U.S. 551, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004) (declining to extend the *Leon* good faith exception to law enforcement officials who issued a warrant that listed only the location of the evidence without describing the items to be seized); *United States v. George*, 975 F.2d 72 (2d Cir. 1992) (declining to extend the good faith exception to a warrant issued following a robbery that included only a list of items, the address subject to search, and the phrase "any other evidence relating to the commission of a crime).

increasingly intrusive searches at Steps Two and Three of Google's process. Instead, the warrant ceded authority and decision-making from an independent judicial officer to a private corporation. No reasonable officer could believe that execution of this geofence warrant in this manner comports with the Fourth Amendment and the liberties it serves to protect. In the same way that this cannot cure the constitutional violation that occurred, *see* Wynn, J. concurring at 35–53 and Berner, J., concurring at 109–13, it does not excuse the officer's indiscretions. Exclusion of the evidence is therefore appropriate here.

One dear colleague suggests that even if there was a search, placing restraints on law enforcement's use of geofence location data and other emerging technologies is unjustified. Wilkinson, J., concurring at 22–23 (stating "[e]ven if there was a search, there is no room for emergent judicial hostility" because such restraint would "frustrate law enforcement's ability to keep pace with tech-savvy criminals" and "[m]ore cold cases would go unsolved"). I am not unmindful of nor insensitive to the number of cases that go unsolved each year and the lack of closure that results from this unfortunate reality. I am, however, vehemently opposed to the notion that new technology erodes the protections and principles of our Constitution. Crimes have gone unsolved due to lack of suspect and witness identification, lack of evidence, and other issues beyond law enforcement control presumably since the beginning of recorded time.

That fact, however, has never justified infringement on the Constitution and as such, should not be used as a reason to withhold Fourth Amendment protections or

excuse Fourth Amendment violations. Indeed, the Supreme Court has said as much. Specifically, the Supreme Court stated "that [t]he efforts of the courts and their officials to bring the guilty to punishment, praiseworthy as they are, are not to be aided by the sacrifice of those great [constitutional] principles." *Mapp v. Ohio*, 367 U.S. 643, 648, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961) (quoting *Weeks v. United States*, 232 U.S. 383, 391–92, 34 S.Ct. 341, 58 L.Ed. 652 (1914)). Simply put, the judiciary may not be a safe harbor to violations of the Fourth Amendment because cold cases—which have always been an unfortunate reality—will continue. This must remain true no matter how well-meaning the investigative officers' intentions. And technological developments nor corporate practices should alter that calculus.

Some of my colleagues suggest that exclusion is not warranted in this case because this Court nor any other court had opined on the validity of geofence warrants at the time of Detective Hylton's application. Thus, they suggest that any error on Detective Hylton's part resulted from the lack of clear direction regarding geofence warrants. But, contrary to that suggestion, an officer need not know the judiciary's view on the use of new technology with the Fourth Amendment to know that the information in the warrant was insufficient. It is well-settled that, to be valid, a warrant must include the particular person, place, or thing to be searched. *Smith*, 442 U.S. at 736 n.2, 99 S.Ct. 2577 (citing U.S. Const. amend. IV). Accordingly, whatever the alleged uncertainty regarding geofence warrants, it was not unclear what the Constitution demands of all warrants. That being the case, the lack of authority regarding

geofence warrants does not end the inquiry into the objective reasonableness of Detective Hylton's conduct. And for good reason, as endorsement of that practice would run the risk of forgiving law enforcement impropriety simply because no court has specifically forbidden it. That is the very type of behavior the Supreme Court cautioned against in the context of retroactivity of Fourth Amendment rulings. Namely, that "police or other courts [would] disregard the plain purport of our decisions and [ ] adopt a let's-wait-until-it's-decided approach." *Leon*, 468 U.S. at 912 n.9, 104 S.Ct. 3405 (citing *U.S. v. Johnson*, 457 U.S. 537, 561, 102 S.Ct. 2579, 73 L.Ed.2d 202 (1982)) (internal quotation marks omitted). If we permitted that course of action, Fourth Amendment protections would become a nullity in the face of rapidly emerging technology.

The same unfortunate fate would result if Detective Hylton's belief in his actions was dispositive. *Leon* instructs us to assess whether the investigating officer held an objectively reasonable belief in the warrant's validity and his actions. 468 U.S. at 919, 104 S.Ct. 3405. Detective Hylton's subjective belief, or what he "could have" believed, then, is therefore of little moment. *Contra* Heytens, J., concurring at 88 (stating "because the investigating officer *could have had* 'an objectively reasonable good-faith belief that his conduct was lawful,' I think the district court was right to withhold 'the harsh sanction of exclusion'") (citing *Davis*, 564 U.S. at 238, 240, 131 S.Ct. 2419) (emphasis added) (internal brackets omitted).

This too makes sense as constitutional rights should not be so subjugated to the will of individual officers. *Leon*,

468 U.S. at 915 n.13, 104 S.Ct. 3405 ("Good faith on the part of the arresting officers is not enough") (citing *Henry v. United States*, 361 U.S. 98, 102, 80 S.Ct. 168, 4 L.Ed.2d 134 (1959)) (internal brackets and quotation marks omitted). If subjective good faith alone were the test, the protections of the Fourth Amendment would evaporate, and the people would be "'secure in their persons, houses, papers, and effects,' only in the discretion of the police." *Id.*

Similarly, it is a perilous day when our Fourth Amendment protections lie in the hands of a private company, and constitutional rights should not and cannot be defined by the internal policies of a private corporation. This is so even where the process was created with input from law enforcement. To that point, I note that the government and some of my colleagues highlight that Google's process was created in conjunction with the Department of Justice. Notably, the government's interest in defining the Fourth Amendment right is no greater than that of the defense counsel, other attorneys, and the public at large—none of whom were offered a seat at the table. And, even if Google had opened the forum to all potential stakeholders, its process would still lack finality because corporations lack the authority to interpret the Constitution. That responsibility belongs to the courts, and we must not relinquish it to those not charged with protecting the Constitution or otherwise abdicate it because the task seems too difficult.

II.

Law enforcement should not be denied the benefit of the efficiencies that emerging technologies offer. However, when seeking digital evidence, officers must demonstrate at least the same level of supporting information necessary to justify the search of physical places and things. In other words, officers should not be permitted, with aid of an unbridled warrant, to shake the proverbial digital tree without an objectively reasonable belief that the warrant and the manner of its execution are consistent with the Fourth Amendment. And that reasonable belief must be founded on something more than the commonality of the technology at issue in the case. This is especially so given that technology has and continues to shift our understanding of "person, place, or thing."

Some cry "novelty" and "technological change" as an excuse for a fundamental departure from our constitutional principles. But one thing is for certain: technology will continue to shift, but the basic protections of the Fourth Amendment must remain. The people's rights against unreasonable searches and seizures cannot not bend to accommodate the volatility of technology. Rather, new technologies must bend to accomplish the vitality of the protections guaranteed to the people under the Fourth Amendment. Regrettably, the ever-increasing extension of the good faith exception to the exclusionary rule has turned this sacred principle of Fourth Amendment interpretation on its head.

The Constitution nor Fourth Amendment precedent to date anticipated that person may one day refer to a non-

human, such as Optimus; places could encompass locations in the Metaverse (or otherwise only digitally accessible); and things could include intangible objects that exist only electronically. Given that reality, the judiciary still must fulfill its role and duty to ensure that the interpretation of the Constitution does not fall solely in the hands of anyone not charged with protecting the rights it guarantees. Our Court failed to do so here. Thus, I must dissent.

Appendix B

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

No. 22-4489
(3:19-cr-00130-MHL-1)

UNITED STATES of America,

Plaintiff – Appellee,

v.

Okello T. CHATRIE,

Defendant – Appellant.

The Reporters Committee for Freedom of the Press; American Civil Liberties Union; American Civil Liberties Union of Virginia; Eight Federal Public Defender Offices Within the Fourth Circuit; Technology Law and Policy Clinic at New York University School of Law; Electronic Frontier Foundation,

Amici Supporting Appellant.

Project for Privacy and Surveillance Accountability, Inc.,

Amicus Supporting Rehearing Petition.

|

FILED: November 1, 2024

ORDER

A majority of judges in regular active service and not disqualified having voted in a requested poll of the court to grant the petition for rehearing en banc,

IT IS ORDERED that rehearing en banc is granted. The parties shall file 16 additional paper copies of their briefs and appendices previously filed in this case within 10 days. The case shall be scheduled at the next available session.

For the Court

/s/ Nwamaka Anowi, Clerk

Appendix C

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

No. 22-4489

UNITED STATES of America,

Plaintiff – Appellee,

v.

Okello T. CHATRIE,

Defendant – Appellant.

The Reporters Committee for Freedom of the Press; American Civil Liberties Union; American Civil Liberties Union of Virginia; Eight Federal Public Defender Offices Within the Fourth Circuit; Technology Law and Policy Clinic at New York University School of Law; Electronic Frontier Foundation,

Amici Supporting Appellant.

Project for Privacy and Surveillance Accountability, Inc.,

Amicus Supporting Rehearing Petition.

Argued: December 8, 2023

Decided: July 9, 2024

Before WILKINSON, WYNN, and RICHARDSON, Circuit Judges.

Affirmed by published opinion. Judge Richardson wrote the opinion, in which Judge Wilkinson joined. Judge Wynn wrote a dissenting opinion.

ARGUED: Michael William Price, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, Washington, D.C., for Appellant. Nathan Paul Judish, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellee. **ON BRIEF:** Geremy C. Kamens, Federal Public Defender, Alexandria, Virginia, Laura J. Koenig, Assistant Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Richmond, Virginia, for Appellant. Kenneth A. Polite, Jr., Assistant Attorney General, Richard W. Downing, Deputy Assistant Attorney General, Computer Crime and Intellectual Property Section, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C.; Jessica D. Aber, United States Attorney, Kenneth R. Simon, Jr., Assistant United States Attorney, Peter S. Duffey, Assistant United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Richmond, Virginia, for Appellee. Jennifer Lynch, Andrew Crocker, Hannah Zhao, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California; Jacob M. Karr, Technology Law and Policy Clinic, NEW YORK UNIVERSITY SCHOOL OF LAW, New York, New York, for Amici Technology Law and Policy Clinic at New York University School of Law and Electronic Frontier Foundation. Jennifer Stisa Granick, San Francisco, California, Nathan Freed Wessler, Ashley

Gorski, Patrick Toomey, Brandon Buskey, Trisha Trigilio, Laura Moraff, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York; Eden B. Heilman, Matthew W. Callahan, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA, Richmond, Virginia; William F. Nettles, IV, Federal Public Defender, Columbia, South Carolina, G. Alan DuBois, Federal Public Defender, Raleigh, North Carolina, Louis Allen, Federal Public Defender, Greensboro, North Carolina, Juval O. Scott, Federal Public Defender, Roanoke, Virginia, Brian J. Kornbrath, Federal Public Defender, Clarksburg, West Virginia, James Wyda, Federal Public Defender, Baltimore, Maryland, Wesley P. Page, Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Charleston, West Virginia; John Baker, Federal Public Defender, FEDERAL DEFENDERS OF WESTERN NORTH CAROLINA, INC., Charlotte, North Carolina, for Amici American Civil Liberties Union, American Civil Liberties Union of Virginia, and Eight Federal Public Defender Offices Within the Fourth Circuit. Bruce D. Brown, Katie Townsend, Gabe Rottman, Grayson Clary, Emily Hockett, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, Washington, D.C., for Amicus Reporters Committee for Freedom of the Press.

RICHARDSON, Circuit Judge:

Okello Chatrie appeals the district court's denial of his motion to suppress location data obtained using a geofence warrant. He argues that the geofence warrant violated the Fourth Amendment because it lacked probable cause and particularity. But we find 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. We therefore affirm the district court.

I. Background

This case involves government access to a specialized form of location information maintained by Google. Understanding the nature of this information, how it is generated, and how Google obtains it is necessary to our disposition. Accordingly, we begin with a description of the relevant technology.[1]

A. Google Location History and Geofence Warrants

Few readers need an introduction to Google, the technology supergiant that offers products and services like Android, Chrome, Google Search, Maps, Drive, and Gmail. This case, however, is about a particular setting for mobile devices that Google calls "Location History."

Location History is an optional account setting that allows Google to track a user's location while he carries

---

[1] After we held argument for this case, Google announced changes to its Location History setting. *See* Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, Google (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps/ [https://perma.cc/Y62G-GBUW]. In this opinion, we describe Location History as the record reflects that it existed when the government obtained Chatrie's information in 2019. We do not opine on how Google's changes will affect future cases.

his mobile devices. If a user opts in, Google keeps a digital log of his movements and stores this data on its servers. Google describes this setting as "primarily for the user's own use and benefit." J.A. 131. And enabling it does unlock several useful features for a user. For instance, he can view a "virtual journal" of his past travels in the "Timeline" feature of the Google Maps app. J.A. 128. He can also obtain personalized maps and recommendations, find his phone if he loses it, and receive real-time traffic updates. But Google uses and benefits from a user opting in, too—mostly in the form of advertising revenue. Google uses Location History to show businesses whether people who viewed an advertisement visited their stores. It similarly allows businesses to send targeted advertisements to people in their stores' proximity.

Location History is turned off by default, so a user must take several affirmative steps before Google begins tracking and storing his Location History data. First, he must enable location sharing on his mobile device.[2] Second, he must opt in to the Location History setting on his Google account, either through an internet browser, a Google application (such as Google Maps), or his device settings (for Android devices). Before he can activate the setting, however, Google always presents him language that explains the basics of the service.[3]

---

[2] For iOS devices, he must also grant location permission to applications capable of using that information.

[3] This text is the same no matter how a user opts in to Location History. It explains that Location History "[s]aves where you go with your devices," and that "[t]his data may be saved and used in any Google service where you were signed in to give you more

Third, he must enable the "Location Reporting" feature on his mobile device.[4] And fourth, he must sign in to his Google account on that device. Only when a user follows these steps will Google begin tracking and storing his Location History data. Roughly one-third of active Google users have enabled Location History.

Even after a user opts in, he maintains some control over his location data. He can review, edit, or delete any information that Google has already obtained. So, for instance, he could decide he only wants to keep data for certain dates and to delete the rest. Or he could decide to delete everything. Google also allows him to pause (*i.e.*, disable) the collection of future Location History data.[5] Whatever his choice, Google will honor it. From start to finish, then, the user controls how much Google tracks and stores his Location History data.

---

personalized experiences. You can see your data, delete it and change it in your settings at account.google.com." J.A. 1564. It also presents an expansion arrow, which, if tapped by the user, displays more information about Location History. For instance, it explains that "Google regularly obtains location data from your devices ... even when you aren't using a specific Google service." J.A. 1565.

[4] Location Reporting allows a user to control which devices in particular will generate Location History information. So a user could enable Location History at the account level but then disable Location Reporting for a particular device. That device then would not generate Location History data.

[5] Additionally, if a user disables location sharing on his device, that device will cease sharing location information with Location History, even if Location History and Location Reporting remain enabled.

Once a user enables Location History, Google constantly monitors his location through GPS, even when he isn't using his phone.[6] And if he has an Android phone, he can turn on another setting—"Google Location Accuracy"—that enables Google to determine his location using more inputs than just GPS, such as Wi-Fi access points and mobile networks. As a result, Location History can be more precise than other location-tracking mechanisms, including cell-site location information. But whether Google Location Accuracy is activated or not, Location History's power should not be exaggerated. In the end, it is only an estimate of a device's location. So when Google records a set of location coordinates, it includes a value (measured in meters) called a "confidence interval," which represents Google's confidence in the accuracy of the estimate.[7] Google represents that for any given location point, there is a 68% chance that a user is somewhere within the confidence interval.

Google stores all Location History data in a repository called the "Sensorvault." The Sensorvault assigns each device a unique identification number and maintains all Location History data associated with that device. Google then uses this data to build aggregate models to assist applications like Google Maps.

In 2016, Google began receiving "geofence warrants" from law enforcement seeking to access location information. A geofence warrant requires Google to

---

[6] On average, Google logs a device's location every two minutes.

[7] For example, if the confidence interval is one hundred meters, then Google estimates that a user is likely within a one-hundred-meter radius of the coordinates.

produce Location History data for all users who were within a geographic area (called a geofence) during a particular time period.[8] Since 2016, geofence requests have skyrocketed in number: Google claims it saw a 1,500% increase in requests from 2017 to 2018 and a 500% increase from 2018 to 2019. Concerned with the potential threat to user privacy, Google consulted internal counsel and law enforcement agencies in 2018 and developed its own three-step procedure for responding to geofence requests. Since then, Google has objected to any geofence request that disregards this procedure.

Google's procedure works as follows: At Step One, law enforcement obtains a warrant that compels Google to disclose an anonymous list of users whose Location History shows they were within the geofence during a specified timeframe. But Google does not keep any lists like this on-hand. So it must first comb through its entire Location History repository to identify users who were present in the geofence. Google then gives law enforcement a list that includes for each user an anonymized device number, the latitude and longitude coordinates and timestamp of each location point, a confidence interval, and the source of the stored Location History (such as GPS or Wi-Fi). Before disclosing this information, Google reviews the request and objects if Google deems it overly broad.

---

[8] Geofence warrants seek only Location History data and no other forms of location information, so they only affect people who had this feature enabled at the requested time and place.

At Step Two, law enforcement reviews the information it receives from Google. If it determines that it needs more, then law enforcement can ask Google to produce additional location coordinates. This time, the original geographical and temporal limits no longer apply; for any user identified at Step One, law enforcement can request information about his movements inside and outside the geofence over a broader period. Yet Google generally requires law enforcement to narrow its request for this more expansive location data to only a subset of the users pinpointed in Step One.

Finally, at Step Three, law enforcement determines which individuals are relevant to the investigation and then compels Google to provide their account-identifying information (usually their names and email addresses). Here, too, Google typically requires law enforcement to taper its request from the previous step, so law enforcement can't merely request the identity of every user identified in Step Two.

B. Facts

On May 20, 2019, someone robbed the Call Federal Credit Union in Midlothian, Virginia. The suspect carried a gun and took $195,000 from the bank's vault. He then fled westward before police could respond.

The initial investigation into the robbery proved unfruitful. When Detective Joshua Hylton arrived at the scene, he interviewed witnesses and reviewed the bank's security footage. But these failed to reveal the suspect's identity. And after chasing down two dead-end leads, Detective Hylton seemed to be out of luck.

Yet there was one thing Detective Hylton still hadn't tried. He saw on the security footage that the suspect had carried a cell phone during the robbery. In the past, Detective Hylton had sought and obtained three separate geofence warrants after consulting prosecutors. So on June 14, 2019, he applied for and obtained a geofence warrant from the Chesterfield County Circuit Court of Virginia.

The warrant drew a geofence with a 150-meter radius covering the bank. It then laid out the three-step process by which law enforcement would obtain location information from Google. At Step One, Google would provide anonymized Location History information for all devices that appeared within the geofence from thirty minutes before to thirty minutes after the bank robbery. This information would include a numerical identifier for each account. At Step Two, law enforcement would "attempt[ ] to narrow down that list" to a smaller number of accounts and provide the narrowed list to Google. J.A. 116. Google would then disclose anonymized location data for all those devices from one hour before to one hour after the robbery. But unlike the Step One information, the Step Two information would be unbounded by the geofence. Finally, at Step Three, law enforcement would again attempt to shorten the list, and Google would provide the username and other identity information for the requested accounts.

In response to the warrant, Google first provided 209 location data points from nineteen accounts that appeared within the geofence during the hour-long period. Detective Hylton then requested Step Two information from nine accounts identified at Step One.

Google responded by producing 680 data points from these accounts over the two-hour period. Finally, Detective Hylton requested the subscriber information for three accounts, which Google provided. One of these accounts belonged to Okello Chatrie.[9]

C. Procedural History

On September 17, 2019, a grand jury in the Eastern District of Virginia indicted Chatrie for (1) forced accompaniment during an armed credit union robbery, in violation of 18 U.S.C. §§ 2113(a), (d), and (e); and (2) using, carrying, or brandishing a firearm during and in relation to a crime of violence, in violation of § 924(c)(1)(A). Chatrie was arraigned on October 1, 2019, and pleaded not guilty. He then moved to suppress the evidence obtained using the geofence warrant.

On March 3, 2022, the district court denied Chatrie's motion to suppress. Although the court voiced concern about the threat geofence warrants pose to user privacy, it declined to resolve whether the geofence evidence was obtained in violation of the Fourth Amendment. Rather, 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, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).

---

[9] According to Google's records, Chatrie created a Google account on August 20, 2017. He later opted in to Location History from a Samsung smartphone on July 9, 2018.

Chatrie subsequently entered a conditional guilty plea and was sentenced to 141 months' imprisonment and 3 years' supervised release. This timely appeal followed.

II. Discussion

On appeal, Chatrie asks us to hold that the geofence warrant violated his Fourth Amendment rights and that the fruits of the warrant should be suppressed. He argues that the government conducted a Fourth Amendment search because it invaded his reasonable expectation of privacy in his location information. He further claims that the geofence warrant authorizing the search was invalid for lack of probable cause and particularly. Finally, he asserts that the good-faith exception to the exclusionary rule does not apply to this warrant.

The district court denied Chatrie's motion to suppress based on the good-faith exception. We agree that the motion should be denied, but for a different reason: Chatrie did not have a reasonable expectation of privacy in two hours' worth of Location History data voluntarily exposed to Google. So the government did not conduct a search when it obtained this information from Google. We therefore affirm the district court's decision. *See United States v. Smith*, 395 F.3d 516, 519 (4th Cir. 2005) (holding that we may affirm a district court "on any grounds apparent from the record").

A. *Carpenter*, *Beautiful Struggle*, and the Third-Party Doctrine

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. To trigger its protections, the government must conduct a "search" (or "seizure") covered by the Fourth Amendment. "For much of our history, Fourth Amendment search doctrine was 'tied to common-law trespass' and focused on whether the government 'obtains information by physically intruding on a constitutionally protected area.'" *Carpenter v. United States*, 585 U.S. 296, 304, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018) (quoting *United States v. Jones*, 565 U.S. 400, 405, 406 n.3, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012)). This trespass-based approach remains alive and well to this day. *See, e.g.*, *Jones*, 565 U.S. at 405–08, 132 S.Ct. 945.

But as American society changed and technology developed, so too did the government's ability to intrude on sensitive areas. *Carpenter*, 585 U.S. at 305, 138 S.Ct. 2206. So the Supreme Court birthed a new privacy-based framework in *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). Under *Katz*, a search occurs when the government invades an individual's reasonable expectation of privacy. *Id.* at 351, 88 S.Ct. 507; *id.* at 360, 88 S.Ct. 507 (Harlan, J., concurring); *see also Smith v. Maryland*, 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). This privacy-based approach augments the prior trespass-based approach by providing another way to identify a Fourth Amendment

search. *See Jones*, 565 U.S. at 405–08, 132 S.Ct. 945; *Carpenter*, 585 U.S. at 304, 138 S.Ct. 2206.

Though sweeping, *Katz*'s reasonable-expectation framework is not boundless. One important limit on its scope is the "third-party doctrine." The Supreme Court has long recognized that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743–44, 99 S.Ct. 2577. This is because he "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *United States v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). And it holds true "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* Thus, in *United States v. Miller*, the Court held that the government did not conduct a search when it obtained an individual's bank records from his bank, since he voluntarily exposed those records to the bank in the ordinary course of business. *Id.* at 443, 96 S.Ct. 1619. Likewise, in *Smith v. Maryland*, the Court held that the government did not conduct a search when it used a pen register to record outgoing phone numbers dialed from a person's telephone, because he voluntarily conveyed those numbers to his phone company when placing calls. 442 U.S. at 742, 99 S.Ct. 2577.[10]

---

[10] Of course, *Miller* and *Smith* were not the only cases to invoke this principle. The Court has applied the third-party doctrine to other kinds of information, too, including incriminating conversations with undercover agents, *United States v. White*, 401 U.S. 745, 749–52, 91 S.Ct. 1122, 28 L.Ed.2d 453 (1971), and tax documents given to

Despite its clear mandate, the third-party doctrine has proved difficult to implement in the digital age. After all, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417, 132 S.Ct. 945 (Sotomayor, J., concurring). If they lack Fourth Amendment protections for any electronically shared data, then the government could access whole swaths of private information free from constitutional scrutiny.

The Court addressed this tension in a series of cases involving the government's use of location-tracking technology. First, in *United States v. Knotts*, the Court held that the government did not conduct a search when it placed a tracking device in a container purchased by one of Knotts's co-conspirators and used it to monitor his short trip to Knott's cabin. 460 U.S. 276, 278–80, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983). The Court explained that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," since he "voluntarily convey[s] [them] to anyone who want[s] to look." *Id.* at 281, 103 S.Ct. 1081. The use of the tracker merely "augment[ed]" existing police capabilities and "amounted principally to the following of an automobile on public streets and highways." *Id.* at 281–82, 103 S.Ct. 1081. Yet the Court reserved whether it would treat

---

an accountant, *Couch v. United States*, 409 U.S. 322, 335, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973).

long-term surveillance differently. *Id.* at 283–84, 103 S.Ct. 1081.[11]

---

[11] Separately, the Court held that police did not conduct a search when they observed the beeper on the premises of Knotts's cabin. *Knotts*, 460 U.S. at 284–85, 103 S.Ct. 1081. "[T]here is no indication," the Court explained, "that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin." *Id.* at 285, 103 S.Ct. 1081. So the government did not invade Knott's reasonable expectation of privacy in his home when it observed the beeper on his property.

Yet the Court reached the opposite result one year later in *United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984). *Karo*, like *Knotts*, involved police use of a beeper to monitor the movement of a container; only this time, officers used it to determine whether the container remained inside a home rented by several of the defendants. *Id.* at 709–10, 104 S.Ct. 3296. The Court held that this use of the beeper "violate[d] the Fourth Amendment rights of those who ha[d] a justifiable interest in the privacy of the residence." *Id.* at 714, 104 S.Ct. 3296. The beeper allowed the government to obtain information that it otherwise could not have obtained—that the item was still inside the house—without entering the home itself, which would have required a warrant. *Id.* at 715, 104 S.Ct. 3296. It therefore intruded on the reasonable expectation of privacy of all who had a Fourth Amendment interest in that home. *Id.* at 719, 104 S.Ct. 3296 (ruling that the evidence was inadmissible against "those with privacy interests in the house"); *see also Kyllo v. United States*, 533 U.S. 27, 40, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."); *but see Karo*, 468 U.S. at 716 n.4, 104 S.Ct. 3296 (distinguishing *Rawlings v. Kentucky*, 448 U.S. 98, 100 S.Ct. 2556, 65 L.Ed.2d 633 (1980), since the defendant in that case did not have a reasonable expectation of privacy in the place searched).

This issue later resurfaced in *United States v. Jones*, 565 U.S. 400, 132 S.Ct. 945. There, the government attached a GPS device to Jones's automobile and used it to track his movements for twenty-eight days. *Id.* at 402–04, 132 S.Ct. 945. Applying the original property-based approach, the Court decided that the government's physical trespass on Jones's vehicle amounted to a search. *Id.* at 404–05, 132 S.Ct. 945. But in separate opinions, five Justices would have held that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"—even though a person's movements are seemingly shared with third parties. *Id.* at 430, 132 S.Ct. 945 (Alito, J., concurring in the judgment); *id.* at 415, 132 S.Ct. 945 (opinion of Sotomayor, J.). Such long-term monitoring violates reasonable expectations of privacy because "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 430, 132 S.Ct. 945 (opinion of Alito, J.).

After *Jones*, it was unclear how the Court would decide a case involving long-term monitoring without a physical trespass. The Court eventually considered this issue in *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206. *Carpenter* involved government access to historical cell-site location information ("CSLI")—a time-stamped record that is automatically generated every time any cell phone connects to a cell site. *Id.* at 300–01, 138 S.Ct. 2206. The government requested—without a warrant—7 days' worth of Carpenter's historical CSLI from one wireless carrier and 152 days' worth from another. *Id.* at

302, 138 S.Ct. 2206.[12] It then used this information to tie him to the scene of several robberies. *Id.* Carpenter moved to suppress the evidence, arguing that the government had conducted a search without a warrant. *Id.*

The Court began by noting that government access to CSLI "does not fit neatly under existing precedents" but "lie[s] at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake." *Id.* at 306, 138 S.Ct. 2206. Starting with the location-tracking cases, the Court found that CSLI "partakes of many of the qualities"—and in some ways, exceeds them—"of the GPS monitoring we considered in *Jones*." *Id.* at 309–13, 138 S.Ct. 2206. The unprecedented surveillance capabilities afforded by CSLI, retrospective over days, reveal—directly and by deduction—a broad array of private information. *Id.* at 310–12, 138 S.Ct. 2206. The Court thus explained that CSLI provides law enforcement "an all-encompassing record of the holder's whereabouts" over that period, *id.* at 311, 138 S.Ct. 2206, allowing it to peer into a person's "privacies of life," including "familial, political, professional, religious, and sexual associations." *Id.* (first quoting *Riley v. California*, 573 U.S. 373, 403, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014); and then quoting *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (opinion of Sotomayor, J.)). Such access—at least, to 7 days' worth of CSLI—invades the reasonable expectation of privacy

[12] Although the government requested 7 days' worth of CSLI from one wireless carrier and 152 days' worth from the other, it received only 2 days' worth from the former and 127 days' worth from the latter. *Carpenter*, 585 U.S. at 302, 138 S.Ct. 2206.

individuals have "in the whole of their physical movements." *Id.* at 310 & n.3, 138 S.Ct. 2206.

That Carpenter "shared" his CSLI with his wireless carriers didn't change the Court's conclusion. *Id.* at 314, 138 S.Ct. 2206. Rejecting the government's invocation of the third-party doctrine, the Court found that the rationales that historically supported the doctrine did not apply to CSLI. *Id.* It first considered "'the nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'" *Id.* (quoting *Miller*, 425 U.S. at 442, 96 S.Ct. 1619). And it found that, unlike the bank records in *Miller* or the pen register in *Smith*, CSLI is extremely revealing of a person's private life. *Id.* at 314–15, 138 S.Ct. 2206 (noting that CSLI is a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years"). The government's access of this information therefore "implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Id.* at 315, 138 S.Ct. 2206.

The Court then found that Carpenter did not *voluntarily* expose this "comprehensive dossier of his physical movements" to his wireless carriers. *Id.* Rather, "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." *Id.* Put differently, having and operating a cell phone automatically and necessarily requires the transmission of one's CSLI to the wireless carrier. And cell phones "are 'such a pervasive and insistent part of daily life,'" the Court explained, "that carrying one is indispensable to participation in modern society." *Id.* (quoting *Riley*, 573 U.S. at 385, 134 S.Ct.

2473). So "in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over" this information. *Id.* (second alteration in original) (quoting *Smith*, 442 U.S. at 745, 99 S.Ct. 2577). The Court thus declined to extend the third-party doctrine to overcome Carpenter's Fourth Amendment protection. *Id.*

The Court emphasized that its holding was "a narrow one." *Id.* at 316, 138 S.Ct. 2206. It did not decide how the Fourth Amendment applies to other forms of data collection, like real-time (as opposed to historical) CSLI or "tower dumps" (*i.e.*, records of phones connected to a particular cell tower over a given period). *Id.* Nor did it jettison the third-party doctrine's application in other contexts. *Id.* All it held was that the government's acquisition of at least 7 days' worth of historical CSLI is a search within the meaning of the Fourth Amendment. *Id.* at 310 n.3, 316, 138 S.Ct. 2206.[13]

Three years later, we clarified the scope of *Carpenter*'s holding in *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021) (en banc). *Beautiful Struggle* involved a Fourth Amendment challenge to the City of Baltimore's aerial-surveillance program. *Id.* at 333. The program captured aerial photos of thirty-two square city miles every second for "at least 40 hours a week, obtaining an estimated twelve hours of coverage

---

[13] The dissent reads *Carpenter* to hold that access to just 2 days' worth of CSLI is a search. Diss. Op. at 354. But even though one of the wireless carriers produced only 2 days' worth of CSLI in response to the government's request for 7 days' worth, *Carpenter* only held that "accessing *seven days* of CSLI constitutes a Fourth Amendment search." *Carpenter*, 585 U.S. at 310 n.3, 138 S.Ct. 2206 (emphasis added).

of around 90% of the city each day." *Id.* at 334. We interpreted *Carpenter* to "solidif[y] 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 (second alteration in original) (quoting *Carpenter*, 585 U.S. at 310, 138 S.Ct. 2206). And we held that Baltimore's program crossed that line because it afforded the government retroactive access to a "detailed, encyclopedic" record of every person's movement in the city across days and weeks. *Id.* (quoting *Carpenter*, 585 U.S. at 309, 138 S.Ct. 2206). The sheer breadth of this information "enable[d] deductions about 'what a person does repeatedly, what he does not do, and what he does ensemble,' which 'reveal[s] more about a person than does any individual trip viewed in isolation.'" *Id.* at 342 (second alteration in original) (quoting *United States v. Maynard*, 615 F.3d 544, 562–63 (D.C. Cir. 2010)). So we held that, when it accessed this information, the government intruded on reasonable expectations of privacy and thereby conducted a search. *Id.* at 346.[14]

B. Application

Relying on *Carpenter*, Chatrie argues that the government conducted a search when it obtained his Location History data from Google.[15] We disagree.

---

[14] The government did not invoke the third-party doctrine in *Beautiful Struggle*.

[15] Chatrie does not argue that the government conducted a search when it obtained his subscriber information from Google at Step Three of the geofence warrant process. This is probably because we

Carpenter identified two rationales that justify applying the third-party doctrine: the limited degree to which the information sought implicates privacy concerns and the voluntary exposure of that information to third parties. Both rationales apply here. Accordingly, we find that Chatrie did not have a reasonable expectation of privacy in the two hours' worth of Location History data that law enforcement obtained from Google. So the government did not conduct a search by obtaining it.

Start with the nature of the information sought. *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206. The government requested and obtained only two hours' worth of Chatrie's Location History data.[16] By no means was this an "all-encompassing record of [Chatrie's] whereabouts ... provid[ing] an intimate window into [his] person[al] life." *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206. All the government had was an "individual trip viewed in isolation," which, standing alone, was not

---

have already held that individuals do not have a reasonable expectation of privacy in subscriber information they provide to an internet provider. *See United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010). Chatrie does not ask us to revisit this holding in light of *Carpenter*, so here we consider only whether the government's access of his Location History data was a search.

[16] At argument, Chatrie suggested that the search occurred when *Google* looked through its entire Location History database at the government's behest. But *Carpenter* and *Beautiful Struggle* both held that a search only occurs once the *government* accesses the requested information. *See Beautiful Struggle*, 2 F.4th at 344 ("*Carpenter* was clear on that issue: a search took place 'when the Government *accessed CSLI* from the wireless carriers.'" (quoting *Carpenter*, 585 U.S. at 313, 138 S.Ct. 2206)). So the proper focus of our inquiry is whether the government's access to two hours' worth of Chatrie's Location History data was a search.

enough to "enable[ ] deductions about 'what [Chatrie] does repeatedly, what he does not do, and what he does ensemble.'"[17] *Beautiful Struggle*, 2 F.4th at 342 (quoting *Maynard*, 615 F.3d at 562–63). The information obtained was therefore far less revealing than that obtained in *Jones*, *Carpenter*, or *Beautiful Struggle* and more like the short-term public movements in *Knotts*, which the Court found were "voluntarily conveyed to anyone who wanted to look." *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206 (quoting *Knotts*, 460 U.S. at 281, 103 S.Ct. 1081).[18] A record of a person's single, brief trip is no more revealing than his bank records or telephone call logs. *See Miller*, 425 U.S. at 442, 96 S.Ct. 1619; *Smith*, 442 U.S.

---

[17] Chatrie raises the possibility that a geofence warrant could reveal a person's movements within a constitutionally protected space, like his home. *See Karo*, 468 U.S. at 716–17, 104 S.Ct. 3296; *Kyllo*, 533 U.S. at 40, 121 S.Ct. 2038. The district court expressed similar concerns and noted that the instant geofence warrant included potentially sensitive locations within its radius. But this is an issue for future cases, not the one before us. Chatrie does not contend that the warrant revealed his own movements within his own constitutionally protected space. And to the extent that it might have captured his or others' movements in another person's protected space, Chatrie lacks standing to assert their potential Fourth Amendment claims. *See Rakas v. Illinois*, 439 U.S. 128, 133–34, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978); *Brown v. United States*, 411 U.S. 223, 230, 93 S.Ct. 1565, 36 L.Ed.2d 208 (1973).

[18] Chatrie argues that the amount of information obtained shouldn't matter, given the accuracy with which Location History can estimate a user's location. Yet the question is not whether the government knew with exact precision what Chatrie did on an "individual trip viewed in isolation," *Beautiful Struggle*, 2 F.4th at 342 (quoting *Maynard*, 615 F.3d at 562), but whether it gathered enough information from many trips to "reveal intimate details through habits and patterns," *id.* at 341. That was not the case here.

at 742, 99 S.Ct. 2577. Chatrie thus did not have a "legitimate 'expectation of privacy,'" in the information obtained by the government, so the first rationale for the third-party doctrine applies here. *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206 (quoting *Miller*, 425 U.S. at 442, 96 S.Ct. 1619).

Furthermore, Chatrie voluntarily exposed his location information to Google by opting in to Location History. *Id.* at 315, 138 S.Ct. 2206. Consider again how Location History works. Location History is an optional setting that adds extra features, like traffic updates and targeted advertisements, to a user's experience. But it is "off by default" and must be affirmatively activated by a user before Google begins tracking and storing his location data. J.A. 1333–34. Of course, once Google secures this consent, it monitors his location at all times and across all devices. Yet even then, Google still affords the user ultimate control over how his data is used: If he changes his mind, he can review, edit, or delete the collected information and stop Google from collecting more. Whether Google tracks a user's location, therefore, is entirely up to the user himself. If Google compiles a record of his whereabouts, it is only because he has authorized Google to do so.

Nor is a user's consent secured in ignorance, either. *See Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206 (explaining that the third-party doctrine applies to information "knowingly shared with another"). To the contrary, the record shows that Google provides users with ample notice about the nature of this setting. Before Google allows a user to enable Location History, it first displays text that explains the basics of the service. The text

states that enabling Location History "[s]aves where you go with your devices," meaning "[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences." It also informs a user about his ability to view, delete, or change his location data.[19] A user cannot opt in to Location History without seeing this text.

So unlike with CSLI, a user knowingly and voluntarily exposes his Location History data to Google. First, Location History is not "'such a pervasive and insistent part of daily life' that [activating it] is indispensable to participation in modern society." *Carpenter*, 585 U.S. at 315, 138 S.Ct. 2206 (quoting *Riley*, 573 U.S. at 385, 134 S.Ct. 2473). *Carpenter* found that it is impossible to participate in modern life without a cell phone. *Id.* But the same cannot be said of Location History. While Location History offers a few useful features to a user's experience, its activation is unnecessary to use a phone or even to use apps like Google Maps. Chatrie gives us no reason to think that these added features are somehow indispensable to participation in modern society and that his decision to opt in was therefore involuntary. That two-thirds of active Google users have not enabled Location History is strong evidence to the contrary. *Cf. Riley*, 573 U.S. at 385, 134 S.Ct. 2473 (noting that, as of 2014, "a significant majority of American adults" owned smartphones). Thus, a user can decline to use Location History and still participate meaningfully in modern society.

---

[19] Google provides additional notice of this setting in its Privacy Policy.

Second, unlike CSLI, Location History data is obtained by a user's affirmative act. *Carpenter* noted that "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." 585 U.S. at 315, 138 S.Ct. 2206. But Location History is *off by default* and can be enabled only by a user's affirmative act. A person need not go off the grid by "disconnecting [his] phone from the network ... to avoid" generating Location History data; instead, he can simply decline to opt in and continue using his phone as before. *See id.* Thus, "in [every] meaningful sense," a user who enables Location History "voluntarily 'assume[s] the risk'" of turning over his location information. *Id.* (quoting *Smith*, 442 U.S. at 745, 99 S.Ct. 2577). So the second rationale for the third-party doctrine applies here, too.

The third-party doctrine therefore squarely governs this case. The government obtained only two hours' worth of Chatrie's location information, which could not reveal the privacies of his life. And Chatrie opted in to Location History on July 9, 2018. This means that he knowingly and voluntarily chose to allow Google to collect and store his location information. In so doing, he "t[ook] the risk, in revealing his affairs to [Google], that the information [would] be conveyed by [Google] to the Government." *Miller*, 425 U.S. at 443, 96 S.Ct. 1619. He cannot now claim to have had a reasonable expectation of privacy in this information. *See Smith*, 442 U.S. at

743–44, 99 S.Ct. 2577. The government therefore did not conduct a search when it obtained the data.[20]

---

[20] At argument, Chatrie's counsel argued that this was a search because Chatrie has a property interest in his Location History data. Oral Arg. at 0:30–0:45. But Chatrie forfeited his right to raise this issue on appeal. "It is a well settled rule that contentions not raised in the *argument section of the opening brief* are abandoned." *United States v. Boyd*, 55 F.4th 272, 279 (4th Cir. 2022) (quoting *United States v. Al-Hamdi*, 356 F.3d 564, 571 n.8 (4th Cir. 2004) (emphasis added)); *see also* Fed. R. App. P. 28(a)(8). Chatrie did not advance this claim in the argument section of his opening brief. Instead, he merely alluded to it in a two-sentence footnote that appeared in the *facts section. See* Opening Br. at 14– 15 n.3. Not until his reply brief did Chatrie raise this issue. So Chatrie has forfeited it on appeal.

Even if we found that Chatrie did not forfeit this issue, we would still reject it on the merits. Chatrie does not cite any positive law (state or federal) that gives him an ownership interest in his Location History data. *See Carpenter*, 585 U.S. at 331, 138 S.Ct. 2206 (Kennedy, J., dissenting); *id.* at 353–54, 138 S.Ct. 2206 (Thomas, J., dissenting); *id.* at 402, 138 S.Ct. 2206 (Gorsuch, J., dissenting). Nor does he claim that he could bring a tort suit if this information were stolen. *See id.* at 353, 138 S.Ct. 2206 (Thomas, J., dissenting). Instead, he relies largely on the fact that Google describes Location History as "*your* information," J.A. 39 (emphasis added), and as a user's "virtual journal," J.A. 128. But this is an incredibly thin reed on which to hang such a bold pronouncement. Though we issue no opinion on whether Google can create a property interest merely by saying one exists, Google at least knows how to recognize preexisting property rights when it wants to. At the time Chatrie opted in to Location History, Google explicitly labelled digital cloud content as user property. *See* J.A. 2083 ("You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours."). But Google used no such language to describe its location services. *See* J.A. 2051 (describing location information as content Google "collect[s]" and omitting mention of property rights); J.A.

C. Responding to the Dissent

In our view, this case involves a straightforward application of the third-party doctrine. But the dissent disagrees. Unlike us, the dissent reads *Carpenter* to have abandoned both strands of doctrine that preceded it, at least when the government uses new technology to monitor a person's movements. In their place, the dissent explains, the Court concocted anew a four (or five?) factor balancing test that considers whether police obtained information that was comprehensive, retrospective, intimate, easy to access, and (perhaps?) voluntarily exposed. Diss. Op. at 346–47. The dissent then puts a pot on the fire, combines these ingredients, and *voila!*—finds that the police conducted a search here.

For all its bold pronouncements, the dissent's novel framework only works if you interpret *Carpenter* to have jettisoned both lines of cases that preceded it and created a new inquiry from scratch. Indeed, this thesis seems to undergird the dissent's entire argument, as it repeats it over and over.[21] Contrary to the dissent's

---

1339–40 (omitting mention of property rights at the initial opt-in). We therefore cannot hold, based on the record before us, that Chatrie had a property interest in his Location History data.

[21] *See, e.g.*, Diss. Op. at 345 ("Both lines of cases would seemingly 'inform our understanding of the privacy interests at stake,' ... but neither squarely applies because this kind of data constitutes a 'qualitatively different category' of information ...." (first quoting *Carpenter*, 585 U.S. at 306, 138 S.Ct. 2206; then quoting *id.* at 309, 138 S.Ct. 2206)); *id.* at 345 ("After concluding that no existing Fourth Amendment doctrine applied neatly to such a digital innovation, the *Carpenter* Court applied a new framework based on

claims, however, *Carpenter* did not cast away the decisions that preceded it. Rather, the Court explicitly stated that both the *Knotts-Jones* and the *Smith-Miller* lines of cases "inform our understanding of the privacy interests at stake." 585 U.S. at 306, 138 S.Ct. 2206. It then went on to apply the principles announced in the location-tracking cases, *id.* at 310, 138 S.Ct. 2206, and to distinguish—based on the unique features of CSLI—the third-party cases, *id.* at 313–16, 138 S.Ct. 2206.

Start with *Carpenter*'s treatment of *Jones*. *Carpenter* explained that CLSI "partakes of many of the same qualities of the GPS monitoring that we considered in *Jones*," since it is "detailed, encyclopedic, and effortlessly compiled." *Id.* at 309, 138 S.Ct. 2206. Therefore, the Court held that, as in *Jones*, the government's access to large quantities of this information implicates the reasonable expectation of privacy individuals have in the "whole of their physical movements." *Id.* at 310, 138 S.Ct. 2206.

---

the historical understandings of privacy protections that it had described and concluded that the CSLI obtained 'was the product of a search' that required a warrant." (quoting *Carpenter*, 585 U.S. at 310, 138 S.Ct. 2206)); *id.* at 347 ("Put simply, the Court declined to extend existing doctrines to exempt CSLI from Fourth Amendment protections based on the principle that it first recognized decades earlier: previously unimaginable technology that reveals unprecedented amounts of personal information requires new rules."); *id.* at 347 ("To sum up, the Court concluded that 'personal location information maintained by a third party' lies at the intersection of the public-surveillance and third-party cases, but that neither theory 'neatly' applies." (quoting *Carpenter*, 585 U.S. at 306, 138 S.Ct. 2206)).

Seen in this light, the "factors" identified by the dissent here were not factors at all. They were instead attributes of the large quantity of CSLI obtained by the government that implicated the privacy interest recognized by the concurring Justices in *Jones*. The Court found that access to at least 7 days' worth of Carpenter's CSLI provided a "comprehensive record" of his movements, which revealed intimate details of his life that would not have been knowable if the government only pursued him for a "brief stretch." *Carpenter*, 585 U.S. at 310–11, 138 S.Ct. 2206. And the retrospective nature of CSLI and the ease by which it could be accessed only augmented these privacy concerns, for no comparable record of a person's movements was available to law enforcement in a pre-digital age. *Id.* at 311–12, 138 S.Ct. 2206. In sum, the quantity of CSLI obtained by the government, combined with its immense capabilities, made it akin to the long-term GPS information obtained in *Jones*. So the Court applied established principles and found that Carpenter's CSLI warranted Fourth Amendment protection.

But you don't have to take our word for it. Rather look to our en banc opinion in *Beautiful Struggle*. 2 F.4th 330. *Beautiful Struggle* was our first application of *Carpenter* to novel location-tracking technology. Yet nowhere in that opinion did we suggest that *Carpenter* departed from cases like *Knotts* and *Jones* and created a new, factor-based inquiry. On the contrary, we recognized that "[t]he touchstone in *Carpenter* was the line of cases addressing 'a person's expectation of privacy in [their] physical location and movements,'" *i.e.*, *Knotts* and *Jones*. 2 F.4th at 340 (alteration in original) (quoting

Carpenter, 585 U.S. at 306–07, 138 S.Ct. 2206)). We then explained 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.... The 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. at 341 (alteration in original). Far from recognizing any sort of factor-based inquiry, therefore, *Beautiful Struggle* announced the exact line we draw here—that police invade an individual's reasonable expectation of privacy in the whole of his physical movements when they use technology to monitor his long-term movements, but not when they glimpse only his short-term movements. *See also id.* at 345 ("People 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.... But capturing everyone's movements outside during the daytime for 45 days goes beyond that ordinary capacity.").

Although not couched under this label, *Beautiful Struggle* articulated a version of what one scholar calls the "Mosaic Theory" of the Fourth Amendment. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012). The Mosaic Theory asks whether the government has observed enough of a person's physical movements to deduce

intimate details about his private life that could not be learned from simply observing his isolated trips or activities. Under this theory, access to a person's short-term movements does not invade his reasonable expectation of privacy. Such information reveals only the locations he visits and nothing more, which is something that law enforcement could learn from traditional means of surveillance anyway. *Beautiful Struggle*, 2 F.4th at 341; *Jones*, 565 U.S. at 429, 132 S.Ct. 945 (opinion of Alito, J.). But much more is revealed when the government accesses a larger swath of a person's movements, as this "enables deductions about 'what a person does repeatedly, what he does not do, and what he does ensemble,' which 'reveal[s] more about a person than does any individual trip viewed in isolation.'" *Beautiful Struggle*, 2 F.4th at 342 (alteration in original) (quoting *Maynard*, 615 F.3d at 562–63)). In other words, it exposes "not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206 (quoting *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (opinion of Sotomayor, J.)). Society does not expect that law enforcement would or could gather such a wealth of intimate details about an individual's personal life from his physical movements. *Jones*, 565 U.S. at 430, 132 S.Ct. 945 (opinion of Alito, J.). So when the government crosses that line, it invades a person's reasonable expectation of privacy and conducts a search.[22]

---

[22] The classic explanation of the Mosaic Theory comes from the D.C. Circuit's decision in *United States v. Maynard*, which we quoted extensively when explaining this idea in *Beautiful Struggle*:

The dissent misses *Beautiful Struggle*'s distinction when it catalogues the kind of private details that could be learned from two hours' worth of Location History. According to the dissent, a two-hour snippet of Location History could reveal a wealth of otherwise unknowable and intimate information, like a person's "romantic rendezvous," "medical appointments," or "afternoon and early-evening routines." Diss. Op. at 353. But the theory adopted in *Beautiful Struggle* rejects this exact proposition. To be sure, a two-hour snippet might show that someone visited an apartment, swung by a doctor's office, and then popped into a gym. Yet glimpsing this single trip in isolation could not itself enable sound

---

> The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more.... Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.

Maynard, 615 F.3d at 562; *see Beautiful Struggle*, 2 F.4th at 342 n.8.

deductions about that person's habits, routines, and associations. For example, he may have visited the apartment because he is having an affair, but he equally could have been seeing a friend for coffee, touring a housing upgrade, or buying a couch off of Facebook marketplace. Similarly, he might have visited the doctor's office for his appointment, yet he also could have been dropping off his spouse or collecting information about the doctor's services or needs. And observing someone enter a gym once certainly cannot confirm whether he is a gym rat or simply riding a New Years high. Only by observing that person's movements over a longer period could the police reliably deduce his habits, routines, and associations. No such deductions could accurately be made from a mere two-hour glimpse.[23]

Applying this theory here leads to a straightforward conclusion. As the dissent correctly observes, Location History has capabilities much like GPS data and CSLI. But unlike in *Carpenter* or *Jones*, the government in this case obtained only two hours' worth of Chatrie's Location History data. Although this brief glimpse into his whereabouts may have revealed the locations he visited, it was plainly insufficient to offer insight into his habits, routines, and associations. So the government did not invade his "legitimate 'expectation of privacy'" by

---

[23] The dissent also stresses that law enforcement could deduce the identity of individuals caught within the geofence. Diss. Op. at 353–54. But we fail to see how this is relevant. If law enforcement only observed the short-term movements of everyone caught within the geofence, then it does not matter whether it learned the identity of those people or not—it still did not invade anyone's privacy interest in the whole of their physical movements.

obtaining it.[24] *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206 (quoting *Miller*, 425 U.S. at 442, 96 S.Ct. 1619).

Unable to refute this point, the dissent tries a different tack. The dissent argues that *Beautiful Struggle* and *Knotts* are distinguishable because they involved observation of "strictly ... *public* movements." Diss. Op. at 368. According to the dissent, the duration of the government surveillance is only relevant in cases involving a person's public movements. But this case, unlike *Beautiful Struggle* and *Knotts*, involves technology with the capacity to surveil a person's *private* movements, too. So the dissent would apply a different set of principles here and treat the duration of the intrusion as basically irrelevant.

The dissent is correct that the government conducts a search when it uses sense-enhancing technology to learn information from inside a private space that it could not have learned without physically intruding on that space. *See Kyllo*, 533 U.S. at 34, 121 S.Ct. 2038; *Karo*, 468 U.S. at 713–18, 104 S.Ct. 3296. But the dissent fails to mention

---

[24] We recognize that the theory we apply could lead to hard line-drawing problems in other cases. Some scholars have criticized the Mosaic Theory on precisely these grounds. *See, e.g.*, Kerr, *The Mosaic Theory of the Fourth Amendment*, at 343–53. Indeed, both members of today's majority disagreed with the application of this theory in *Beautiful Struggle* itself. *See* 2 F.4th at 359–62 (Wilkinson, J., dissenting). But regardless of any flaws inherent in this approach, it is the established doctrine of our Circuit. We must apply it as faithfully as we can. And if this theory is to have any meaning, then at the very least it must entail that police observation of a person's two-hour public foray cannot be a search under the Fourth Amendment. Any other result would render the principle announced in *Beautiful Struggle* meaningless.

that those cases involved challenges brought by people who had a reasonable expectation of privacy *in the place searched*. *Kyllo*, 533 U.S. at 29–31, 121 S.Ct. 2038; *Karo*, 468 U.S. at 714, 104 S.Ct. 3296 ("This case thus presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights *of those who have a justifiable interest in the privacy of the residence*.... [W]e think that it does." (emphasis added)). By contrast, the Supreme Court has long held that someone who does not have a Fourth Amendment interest in the place or thing searched lacks standing to challenge that search. *Rawlings*, 448 U.S. at 104–06, 100 S.Ct. 2556; *see Karo*, 468 U.S. at 716 n.4, 719, 104 S.Ct. 3296 (distinguishing *Rawlings* because several defendants had a privacy interest in the place searched, unlike in *Rawlings*). So to challenge the government's use of technology to invade a protected space, a defendant must prove that the government violated *his* reasonable expectation of privacy in that space. The mere fact that the government observed him behind closed doors is insufficient to confer Fourth Amendment standing.

Chatrie does not allege that the Location History data obtained by the government invaded his constitutionally protected space, like his home.[25] And to the extent that

---

[25] Again, we take no position on whether this would be a search, since this issue is not properly presented here. But we do note that the answer isn't as obvious as the dissent represents that it would be. *Compare Karo*, 468 U.S. at 713–18, 104 S.Ct. 3296, *with California v. Ciraolo*, 476 U.S. 207, 213, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) (holding that no search occurs when officers use technology to peer into a person's curtilage if the person knowingly

it may have showed him or others in *someone else's* protected space, Chatrie lacks standing to assert that person's potential Fourth Amendment rights. The dissent may be willing looking past these basic Fourth Amendment standing principles, but we are not.[26]

Now to the dissent's treatment of the third-party doctrine. The dissent thinks that the Supreme Court abandoned *Smith and Miller*, just like it abandoned *Knotts* and *Jones*. After *Carpenter*, on the dissent's view, voluntary exposure either doesn't matter or, if it does, is just another factor in the overall balancing inquiry.

But *Carpenter* did no such thing. As we have already explained, *Carpenter* did not cast aside everything that came before it and create a new framework for assessing Fourth Amendment violations. Rather, the Court

---

exposes his curtilage's contents to others), *and Lewis v. United States*, 385 U.S. 206, 211, 87 S.Ct. 424, 17 L.Ed.2d 312 (1966) (holding that no search occurs when a person invites someone into his home who turns out to be a law enforcement informant).

[26] Adopting the dissent's sweeping approach would create a bizarre incongruity with other areas of Fourth Amendment doctrine. Under traditional Fourth Amendment principles, if the police physically entered Journey Christian Church without a warrant in search of Chatrie, he would not have standing to challenge that search (assuming he had no privacy interest in the church). But under the dissent's view, if police digitally "entered" that same church via Location History, Chatrie could challenge this as an invasion of his rights. For a view that claims to champion "historical understandings" of the Fourth Amendment, Diss. Op. at 344–45 (quoting *Carpenter*, 585 U.S. at 305, 138 S.Ct. 2206), the dissent's approach actually eviscerates basic and longstanding Fourth Amendment principles.

concluded that access to at least 7 days' worth of CSLI invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements. *Carpenter*, 585 U.S. at 310–13, 138 S.Ct. 2206. It then considered whether the third-party doctrine applied to CSLI and ultimately "decline[d] to extend" it, given the sensitive nature of that information and the fact that it is not voluntarily exposed to wireless carriers. *Id.* at 313–16, 138 S.Ct. 2206. Yet Court did not overturn the third-party doctrine, nor did it rule out the possibility of it applying to other types of information or technology that fit more comfortably within its domain. *Id.* at 316, 138 S.Ct. 2206. And it certainly did not reduce the doctrine to one factor in a totality-of-the-circumstances balancing inquiry.[27]

Here, we find that Chatrie—unlike Carpenter—did voluntarily expose his Location History to Google. So we conclude that the third-party doctrine applies to this case. But the dissent disagrees and identifies three facts that supposedly make Chatrie's disclosure of his

---

[27] The dissent's reading is only plausible because it creatively rearranges *Carpenter* to say something it never did. According to the dissent, *Carpenter* first "declin[ed] to extend the third-party doctrine," Diss. Op. at 345, then applied its "new framework" to recognize Carpenter's privacy interest, *id.* at 345–46, and finally considered voluntariness as a sort of independent factor, *id.* at 346. But this is not at all how the Court proceeded. Rather, it first recognized that access to 7 days' worth of CSLI invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements, 585 U.S. at 310–13, 138 S.Ct. 2206, and then declined to extend the third party doctrine, partly because Carpenter's conveyance of CSLI was not meaningfully voluntary, *id.* at 313–16, 138 S.Ct. 2206.

Location History information not "meaningfully voluntary." Diss. Op. at 356. First, Location History, once enabled, always generates and collects information, so its collection is even more automatic and less voluntary than the CSLI collected in *Carpenter*. Second, many individuals generate Location History data, so they must do so involuntarily. Third, Google does not "meaningfully inform" users of how it collects data or how much data it collects at the opt-in stage. *Id.* at 359. We address each argument in turn, finding none convincing.

First, the dissent confuses the extent to which technology conveys information with whether such conveyance is done voluntarily. *Carpenter* found that CSLI is conveyed "without any affirmative act on the part of the user beyond powering up" his cell phone. 585 U.S. at 315, 138 S.Ct. 2206. Thus, a cell phone conveys such information "automatically" without action on the user's part beyond activating his phone. *Id.* By contrast, a user who merely activates and uses his cell phone will not generate Location History data. He only does so once he takes the affirmative step of opting in to the program and consenting to the collection of such data. So even though Location History, once enabled, is constantly collected, it is only constantly collected because it has first been enabled.[28]

---

[28] Nor is the absence of a "physical conveyance," like those in *Smith* and *Miller*, a meaningful distinction. Diss. Op. at 357. Someone who invites another to follow him around and record his movements has conveyed his location information just as voluntarily as someone

Second, the fact that a large number of active Google users have enabled Location History does not prove that they use this service involuntarily. We agree with the dissent that "the use of technology is not per se voluntary just because the adoption of that technology is not as ubiquitous as the cell phone." Diss. Op. at 357. But the flip-side is also true: The ubiquitous use of a particular technology does not necessarily mean that it is used involuntarily. And absent some explanation for why Location History is "'such a pervasive and insistent part of daily life' that [activating it] is indispensable to participation in modern society," *Carpenter*, 585 U.S. at 315, 138 S.Ct. 2206 (quoting *Riley*, 573 U.S. at 385, 134 S.Ct. 2473), we see no reason to treat it as such.[29]

Finally, Google provides adequate information at the opt-in stage to enable a user to knowingly consent to the collection of his data. Before a user can activate Location History, Google explains that "Location History saves where you go with your devices," that "Google regularly obtains location data from your devices," and that "[t]his data is saved even when you aren't using a specific Google service, like Google Maps or Google search." J.A. 1565. By choosing to opt in, then, a reasonable user

---

who records every movement himself and gives the record to another.

[29] The dissent misunderstands why we emphasize that two-third of active Google users have not enabled Location History. We do not invoke this number because we think there is some numeric threshold of users that a service must surpass to become involuntary. Rather, we only think it shows that if Location History were really essential to participation in modern society, it would be odd that most Google users have not activated this service.

would understand that he gave Google broad authorization to track and save Location History data whenever he goes anywhere with his device, even while he is not using it. A user who accepts those terms cannot later claim he did not knowingly expose his information simply because Google didn't explain *exactly* how accurately it would save where he went or *exactly* how regularly it would obtain location data. *Cf. Smith*, 442 U.S. at 745, 99 S.Ct. 2577 ("The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not[,] in our view, make any constitutional difference."); *Florida v. Jimeno*, 500 U.S. 248, 251, 111 S.Ct. 1801, 114 L.Ed.2d 297 (1991) (holding that officers didn't exceed the scope of consent when suspect told them they could search the entire car and they searched containers within the car).[30]

The dissent warns that courts must exercise "humility" when adapting the Fourth Amendment to modern innovations. Diss. Op. at 373. But it is the dissent that fails to heed its own warning. Instead of faithfully apply established principles to the case before us, the dissent

---

[30] The dissent also laments that pausing and deleting Location History is "easier said than done," Diss. Op. at 359, but its evidence for this proposition is basically nonexistent. Other than alluding to generalized grievances about Location History by members of Congress, the media, and Norway's Consumer Protection Committee, the dissent relies on a single email from a Google employee, who suggested that deleting Location History data might be difficult. But the district court made no finding about "[w]hether the substance of this remark is true or not," J.A. 1342, and, absent any further evidence, there is no way to know whether this remark accurately reflects the difficulty of deleting Location History data.

would have us depart from binding case law and apply a novel, unwieldy multifactor balancing test to reach the dissent's preferred policy outcome. We decline the invitation. Our Fourth Amendment doctrine compels a clear result here. If one thinks that this result is undesirable on policy grounds, those concerns should be taken to Congress.

* * *

The Fourth Amendment is an important safeguard to individual liberty. But its protections are not endless. To transgress its command, the government must first conduct a search. We hold that the government did not conduct a Fourth Amendment search when it accessed two hours' worth of Chatrie's location information that he voluntarily exposed to Google. Thus, the district court's decision must be

AFFIRMED.

WYNN, Circuit Judge, dissenting:

This appeal presents this Court's latest opportunity to consider how the Fourth Amendment applies to police use of new surveillance technologies, particularly in light of the Supreme Court's 2018 decision in *Carpenter v. United States*.

The analysis that follows (1) addresses how the Court's understanding of privacy protections evolved alongside technological developments and how *Carpenter* marked the culmination of that evolution; (2) provides a detailed overview of *Carpenter* to explain the new multifactor test it set forward; (3) applies that test to the Location History intrusion at bar; and (4) concludes that the intrusion *was* a search that triggered the Fourth Amendment's protections.

Finally, in an attempt to address this dissent, the majority provides a lengthy separate part to its opinion, relying on unsupported policy premises to support extrajudicial conclusions rather than addressing the serious substantive issues presented by this appeal. To redirect our focus to the merits of this matter, I have added a final section to this dissenting opinion.

I.

At the heart of this appeal, the majority opinion concludes that the government has a virtually unrestricted right to obtain the Location Data History of every citizen. But I believe the government needs a warrant to obtain such Location History data. And that's something the government itself apparently believed at the time it conducted the respective intrusion, since it sought and obtained a warrant in this matter.[1]

A.

Ratified in 1791, the Fourth Amendment safeguards the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," by generally requiring the government to first obtain a warrant from a neutral judge or magistrate before conducting a search. U.S. Const. amend. IV. Historically, the Supreme Court interpreted the Fourth Amendment with an eye toward its origin as the embodiment of the Framers' desire to protect citizens from the arbitrary searches they endured under British rule. *See Carpenter v. United States*, 585 U.S. 296, 303–04, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018). Consistent with this historical view, early decisions employed the "trespass doctrine," under which only physical intrusions by the government into private spaces constituted Fourth Amendment searches that required

[1] The district court only resolved whether the warrant that the government had obtained was valid. The question of whether an unconstitutional search occurred was not decided by the district court.

a warrant. *Katz v. United States*, 389 U.S. 347, 353, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (internal quotation marks omitted); *see Carpenter*, 585 U.S. at 304, 138 S.Ct. 2206; *Olmstead v. United States*, 277 U.S. 438, 457, 48 S.Ct. 564, 72 L.Ed. 944 (1928) (applying trespass doctrine), *overruled by Katz*, 389 U.S. at 347, 88 S.Ct. 507.

Justice Harlan's concurring opinion in *Katz v. United States* signaled a transition from these early principles to modern Fourth Amendment jurisprudence.[2] His opinion articulated a "reasonable expectation of privacy" standard for what type of surveillance constitutes a Fourth Amendment search. *Katz*, 389 U.S. at 361–62, 88 S.Ct. 507 (Harlan, J., concurring). Under this standard, a Fourth Amendment search occurs if (1) an individual has an actual (subjective) expectation of privacy in some activity, and (2) that expectation is one that society recognizes as objectively reasonable. *Id.* at 361, 88 S.Ct. 507 (Harlan, J., concurring). Hence, any government surveillance that infringes upon a person's reasonable privacy expectation necessitates a warrant. *Katz* thereby expanded the recognized Fourth Amendment protections beyond mere physical intrusions. *Id.* at 353, 88 S.Ct. 507; *accord Desist v. United States*, 394 U.S. 244, 250, 89 S.Ct. 1048, 22 L.Ed.2d 248 (1969) ("*Katz* for the first time explicitly overruled the 'physical penetration' and 'trespass' tests enunciated in earlier decisions of this Court."), *abrogated on other grounds by Griffith v.*

---

[2] Though a concurrence is not binding, the reasonable-expectation-of-privacy test articulated in Justice Harlan's concurrence was adopted by a majority of the Court the following year. *See Terry v. Ohio*, 392 U.S. 1, 9, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968).

Kentucky, 479 U.S. 314, 107 S.Ct. 708, 93 L.Ed.2d 649 (1987).

In the 1970s and 1980s—before the internet age—the Supreme Court placed two key limitations on *Katz*'s expansion of recognized Fourth Amendment protections: the third-party and public-surveillance doctrines. *See Carpenter*, 585 U.S. at 306–09, 138 S.Ct. 2206. Because understanding the nuances of those limitations is essential to understanding the Court's recent decision in *Carpenter*, the Court in *Carpenter* reviewed both lines of cases in some detail, and I do the same here.

The seminal third-party-doctrine cases are *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), and *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). In *Smith*, police used a pen-register device to collect the phone numbers the suspect dialed on his home phone. *Smith*, 442 U.S. at 737–38, 99 S.Ct. 2577. And in *Miller*, police accessed the suspect's bank records, such as checks and deposit slips. *Miller*, 425 U.S. at 437–38, 96 S.Ct. 1619. In those cases, the Supreme Court held that the suspects had no reasonable privacy expectations in the records in question because the documents were unrevealing business records that the suspects had voluntarily conveyed to third parties. *See Smith*, 442 U.S. at 737, 740–42, 99 S.Ct. 2577; *Miller*, 425 U.S. at 442–43, 96 S.Ct. 1619.

The analysis in those cases was twofold and found its roots in Justice Harlan's *Katz* concurrence. First, *Smith* and *Miller* reasoned that individuals have no subjective privacy expectation in the phone numbers they dial or in

their bank records because the "nature of those records" is that they are "business records" that reveal little personal information. *Carpenter*, 585 U.S. at 308–09, 138 S.Ct. 2206 (first citing *Smith*, 442 U.S. at 742–43, 99 S.Ct. 2577; and then citing *Miller*, 425 U.S. at 440–43, 96 S.Ct. 1619). The Court in *Smith*, for instance, stressed the pen registers' "limited capabilities": the pen registers did "not acquire the contents of communications," nor reveal the caller and call recipient's "identities, nor whether the call was even completed." *Smith*, 442 U.S. at 741–42, 99 S.Ct. 2577 (emphasis omitted); *accord Miller*, 425 U.S. at 440, 442, 96 S.Ct. 1619 (stating that the records were "not confidential communications but negotiable instruments ... in commercial transactions").

Second, and relatedly, the Court held in both cases that society did not recognize a "reasonable" (or objective) privacy expectation in such unrevealing business records that individuals voluntarily provide to third parties. *See Carpenter*, 585 U.S. at 309, 138 S.Ct. 2206 ("When Smith placed a call, he voluntarily conveyed the dialed numbers ... by exposing that information ... in the ordinary course of business." (quoting *Smith*, 442 U.S. at 744, 99 S.Ct. 2577 (cleaned up))); *Miller*, 425 U.S. at 443, 96 S.Ct. 1619.

Nevertheless, *Smith* qualified its analysis with an eye toward the future. It specified that, if a day should come when our subjective expectations of privacy change due to "influences alien to well-recognized Fourth Amendment freedoms," then the subjective-expectation requirement would have "no meaningful role" in ascertaining the bounds of the Fourth Amendment. *Smith*, 442 U.S. at 740 n.5, 99 S.Ct. 2577. Instead, "a

normative inquiry would be proper." *Id.* Likewise, Justice Marshall's dissent in *Smith* voiced an argument that *Carpenter* would later echo: disclosure to a phone company or bank is not meaningfully voluntary in modern society. *See id.* at 749–51, 99 S.Ct. 2577 (Marshall, J., dissenting).

In two decisions from the 1980s, the Supreme Court placed a second limitation on *Katz*. This second limitation centers upon differences in how *Katz* applies in *public* versus *private* spaces. In *United States v. Knotts*, the Court held that police did *not* conduct a search for Fourth Amendment purposes when they used a beeper—that is, a radio transmitter ... which emits periodic signals that can be picked up by a radio receiver"—to keep a vehicle in view while they followed behind it "on public thoroughfares" during one trip. *United States v. Knotts*, 460 U.S. 276, 277, 281, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983). The Court reasoned that because the suspect's movements were visible to anyone who wanted to look, police could have obtained the same information without the beeper—by physically following him—so the suspect had no reasonable privacy expectation in those public movements. *Id.* at 281–82, 103 S.Ct. 1081.

In so holding, the Court stressed that the beeper was a rudimentary technology that merely "augment[ed]" the visual "sensory faculties" that officers had at "birth." *Id.* at 282, 285, 103 S.Ct. 1081. Thus, *Knotts* "was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance." *Carpenter*, 585 U.S. at 306, 138 S.Ct. 2206. *Knotts*, like *Smith*, also turned an eye to the future: the

Court presciently qualified that should "twenty-four hour surveillance of any citizen" become "possible," then "different constitutional principles may be applicable." *Id.* at 306–07, 138 S.Ct. 2206 (quoting *Knotts*, 460 U.S. at 283–84, 103 S.Ct. 1081 (cleaned up)).

The Court distinguished *Knotts* in its subsequent decision in *United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984). In that case, police used a beeper to track a container as it moved between private residences and commercial lockers. *Id.* at 708–10, 714, 104 S.Ct. 3296. The Court held that, unlike the public surveillance at issue in *Knotts*, the use of a beeper to surveil activity within a *private* residence—a location closed to public view—constituted a Fourth Amendment search. *Id.* at 714–16, 104 S.Ct. 3296.

The upshot of cases like *Smith*, *Miller*, *Knotts*, and *Karo* was that individuals had Fourth Amendment rights where they had a reasonable expectation of privacy, but that they could forfeit those reasonable privacy expectations by voluntarily conveying a business record to a third party, or by traveling in public where police could use rudimentary tools to surveil them.

However, as technology quickly advanced in the ensuing decades and enabled police to surreptitiously collect unprecedented levels of information, the Supreme Court began curtailing the third-party and public-surveillance doctrines to ensure that the exceptions to the Fourth Amendment's protections did not swallow the whole. In doing so, the Supreme Court ensured that the Fourth Amendment remained a firm bulwark against government overreach.

In *Kyllo v. United States*, the Court held that police use of a thermal-imaging device to monitor heat waves emanating from inside a home is a Fourth Amendment search, even though police deployed the device from a *public* street outside the home. *Kyllo v. United States*, 533 U.S. 27, 32, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). The Court rested its holding on its recognition that, even though the device was deployed in a public space, it nonetheless allowed police to "explore details of the home that would previously have been unknowable without physical intrusion." *Id.* at 40, 121 S.Ct. 2038.

Next, in *United States v. Jones*, the Court grappled with "more sophisticated surveillance of the sort envisioned in *Knotts* and found that different principles did indeed apply." *Carpenter*, 585 U.S. at 307, 138 S.Ct. 2206 (citing *United States v. Jones*, 565 U.S. 400, 404–05, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012)). The *Jones* Court held that the police's installation and use of a Global Positioning System ("GPS") tracking device to monitor the location of a suspect's vehicle for 28 days constituted a search. *Jones*, 565 U.S. at 404, 132 S.Ct. 945. Although Justice Scalia's opinion for the five-justice majority rested only on traditional trespass principles, five other justices authored or joined concurrences concluding that the GPS monitoring was a search under the *Katz* reasonable-expectation-of-privacy test—even though the intrusion only captured *public* movements. *See id.* at 413–18, 132 S.Ct. 945 (Sotomayor, J., concurring); *id.* at 419–26, 132 S.Ct. 945 (Alito, J., concurring in the judgment). The concurring justices noted that, as compared to the one-trip beeper intrusion in *Knotts*, the GPS intrusion in *Jones* was longer in duration and conducted with more precise and comprehensive

technology. *See id.* at 415–16, 132 S.Ct. 945 (Sotomayor, J., concurring); *id.* at 427–30, 132 S.Ct. 945 (Alito, J., concurring in the judgment).

Four concurring justices believed the longer duration of the GPS tracking rendered it a search because it constituted "a degree of intrusion that a reasonable person would not have anticipated" and thus violated reasonable expectations of privacy. *Id.* at 430, 132 S.Ct. 945 (Alito, J., concurring in the judgment). That is, because police employing traditional investigative methods could not typically tail a suspect in public for a month straight like they did using GPS in *Jones*, such investigations violate societal expectations and therefore constitute Fourth Amendment searches. *Id.* at 429–30, 132 S.Ct. 945 ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.").

For the fifth concurring justice, Justice Sotomayor, even a *short-term* GPS search violated a reasonable privacy expectation because the technology's "unique attributes" set it apart from the rudimentary beeper in *Knotts*. *Id.* at 415, 132 S.Ct. 945 (Sotomayor, J., concurring). Most famously, she reasoned that because GPS technology "generates a precise, comprehensive record" of a person's public movements, it "reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," which violates our deepest privacy expectations. *Id.* Justice Sotomayor further pointed out that a short GPS search is cheaper, easier to use, and more concealable than conventional surveillance methods—attributes that allow technologies like GPS to "evade[ ] the ordinary checks

that constrain abusive law enforcement practices." *Id.* at 416, 132 S.Ct. 945. Additionally, she noted, GPS technology permits the government to "store" and "efficiently mine" records of an individual's movements "years into the future." *Id.* at 415, 132 S.Ct. 945. For these reasons, she warned, even a short GPS search could chill First Amendment freedoms and "alter the relationship between citizen and government in a way that is inimical to democratic society." *Id.* at 416, 132 S.Ct. 945 (quotation omitted). Finally, she lamented that the third-party doctrine is "ill suited to the digital age," in which people reveal intimate information during "mundane tasks" without expecting their devices to enable "covert surveillance of their movements." *Id.* at 417 & n.*, 132 S.Ct. 945.

Two years later, the Court again demonstrated its awareness that modern technology calls for a more nuanced Fourth Amendment analysis. In *Riley v. California*, it held that police must obtain a warrant to look through the contents of an arrestee's cell phone during an arrest, even though police may generally conduct brief searches of an arrestee's *person* without a warrant. *Riley v. California*, 573 U.S. 373, 385–86, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014). The Court recognized that a cell phone contains a much greater wealth of sensitive information than would be revealed by a traditional physical search, signaling that privacy rights in digital information must be thought of differently. *Id.* at 395–96, 134 S.Ct. 2473.

Thus, in each of these seminal cases, the Supreme Court grappled with how to maintain constitutional privacy protections against police use of or access to encroaching

technologies. And, in the majority opinions in most of these cases and in the *Jones* concurrences, the Court recognized that traditional Fourth Amendment principles were ill-suited to combating the realities of modern technology.

B.

All this case law, demonstrating the Court's growing recognition of the profound impact of technological advancements on Fourth Amendment rights, led up to the Court's 2018 decision in *Carpenter v. United States*. While building on all that came before it, *Carpenter* marked a "[s]ea [c]hange" in Fourth Amendment jurisprudence as it pertains to "a person's digital information." Matthew Tokson, *The Aftermath of* Carpenter: *An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 Harv. L. Rev. 1790, 1799–1800 (2022) [hereinafter Tokson, *The Aftermath of* Carpenter].

In *Carpenter*, the Court held that a police intrusion into seven days of the defendant's historical cell-site-location-information ("CSLI") records, which produced two days' worth of data, constituted a Fourth Amendment search. *Carpenter*, 585 U.S. at 302, 313, 138 S.Ct. 2206. CSLI records are created when cell phones connect to nearby cell towers, which, in *Carpenter*, occurred at the start and end of the defendant's incoming and outgoing calls. *Id.* at 302, 138 S.Ct. 2206. The cell-site records were maintained by wireless companies, *id.* at 306, 138 S.Ct. 2206, which raised the possibility that the third-party doctrine would apply. And indeed, below, the Sixth Circuit had "held that [the defendant] lacked a

reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers." *Id.* at 303, 138 S.Ct. 2206. In other words, the Sixth Circuit took a view very similar to that of the majority here, asking only whether the information in question had been voluntarily conveyed in some manner to a third party.

But the Supreme Court reversed. In so doing, it acknowledged that the third-party doctrine is an increasingly tenuous barometer for measuring an individual's privacy expectations in the digital era. Instead, the Court laid the foundation for a new, multifactor test to be used to determine whether a government intrusion using digital technologies constitutes a search.

The *Carpenter* Court began by reiterating the *Katz* test: the Fourth Amendment protects against intrusion into the sphere in which an individual has a reasonable expectation of privacy. *Id.* at 304, 138 S.Ct. 2206. It then explained that, while "no single rubric" defines what constitutes a reasonable privacy expectation, the Court's analysis must always be "informed by historical understandings of what was deemed an unreasonable search when the Fourth Amendment was adopted." *Id.* at 304–05, 138 S.Ct. 2206 (cleaned up). These historical understandings, according to the Court, have a few "guideposts": "the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power," "to place obstacles in the way of a too permeating police surveillance," and, most importantly, to "assure preservation of that degree of privacy against

government that existed when the Fourth Amendment was adopted." *Id.* at 305, 138 S.Ct. 2206 (cleaned up).

The Court emphasized that it has kept those "Founding-era understandings in mind" when considering "innovations in surveillance tools." *Id.* Pointing to the examples of *Kyllo* and *Riley*, detailed above, the Court explained that its Fourth Amendment jurisprudence has evolved in step with technological developments: "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to [preserve historical privacy protections]." *Id.* (quoting *Kyllo*, 533 U.S. at 34, 121 S.Ct. 2038) (cleaned up); *see id.* (noting that the Court "rejected in *Kyllo* a 'mechanical interpretation' of the Fourth Amendment" to protect individuals from advancing technology (quoting *Kyllo*, 533 U.S. at 35, 121 S.Ct. 2038)); *id.* (pointing to its "recogni[tion]" in *Riley* that "the 'immense storage capacity' of modern cell phones" rendered a cell phone search fundamentally different from a traditional, physical search of an arrestee's person (quoting *Riley*, 573 U.S. at 393, 134 S.Ct. 2473)).

With that background, the Court turned to consider the CSLI intrusion at bar. It quickly concluded that the sort of digital data at issue—"personal location information maintained by a third party"—"does not fit neatly" into any existing line of Fourth Amendment jurisprudence. *Id.* at 306, 138 S.Ct. 2206. Instead, this data "lie[s] at the intersection" of the third-party doctrine (*Smith* and *Miller*) and public-surveillance cases (*Knotts* and *Jones*). *Id.* Both lines of cases would seemingly "inform our understanding of the privacy interests at stake," *id.*, but

neither squarely applies because this kind of data constitutes a "qualitatively different category" of information, *id.* at 309, 138 S.Ct. 2206.

The Court next summarized those two lines of inapplicable cases, *id.* at 306–09, 138 S.Ct. 2206, and then explicitly "decline[d] to extend" the third-party doctrine to CSLI—even though CSLI data is maintained by third-party companies—because CSLI records are "*qualitatively different*" from the types of information that had been at issue in its earlier third-party cases (such as phone numbers and bank records). *Id.* at 309, 138 S.Ct. 2206 (emphasis added); *see also id.* (noting that police surveillance using CSLI is a "new phenomenon"); *id.* (emphasizing the "unique nature" of CSLI and the "novel circumstances" of the case); *id.* at 313, 138 S.Ct. 2206 (noting "seismic shifts in digital technology"); *id.* at 314, 138 S.Ct. 2206 (calling CSLI a "distinct category of information"); *id.* (stressing that "[t]here is a world of difference" between the *Smith* and *Miller* records and CSLI records); *id.* at 318, 138 S.Ct. 2206 ("CSLI is an entirely different species of business record."). "After all," the Court expounded, "when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying ... not just dialed digits, but a detailed and comprehensive record of the person's movements." *Id.* at 309, 138 S.Ct. 2206.

In so declining to extend the third-party doctrine, the Court rejected the notion that there is "a straightforward application of [that] doctrine" to police use of data like CSLI. *Id.* at 314, 138 S.Ct. 2206. To the contrary, the Court held that applying the third-party doctrine to the CSLI in *Carpenter* would have

constituted "a significant extension of [the doctrine] to a distinct category of information." *Id.* Accordingly, it warned that courts would be remiss to "mechanically" apply old theories like the third-party doctrine to novel records like CSLI. *Id.* ("In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.").

After concluding that no existing Fourth Amendment doctrine applied neatly to such a digital innovation, the *Carpenter* Court applied a new framework based on the historical understandings of privacy protections that it had described and concluded that the CSLI obtained "was the product of a search" that required a warrant. *Id.* at 310, 138 S.Ct. 2206; *see id.* at 309–13, 138 S.Ct. 2206. Though the Court did not state explicitly, "here is the applicable test," it clearly delineated the considerations that compelled its decision. Specifically, the Court identified four primary aspects of CSLI that rendered it "qualitatively different" from the traditional sorts of records sought, and forms of surveillance used, by police—its *comprehensiveness*, its *retrospective* capabilities that allowed for historical tracking, the *intimacy* of the information it reveals, and its *ease of access* (i.e., the cost and efficiency) for police. *Id.* at 309–13, 138 S.Ct. 2206. Because those four considerations rendered CSLI unique and violated historical understandings of Fourth Amendment protections, the Court concluded that the suspect maintained a reasonable privacy expectation in his CSLI data, and so the intrusion constituted a Fourth Amendment search. *Id.* at 313, 138 S.Ct. 2206.

In so holding, the Court's analysis followed the reasoning of the concurrences in *Jones*, which likewise argued that the GPS intrusion in that case was a search not due to trespass, but because it violated historical privacy expectations. *E.g.*, *id.* at 310–11, 138 S.Ct. 2206 (first citing *Jones*, 565 U.S. at 430, 132 S.Ct. 945 (Alito, J., concurring in judgment); and then citing *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (Sotomayor, J., concurring)). The *Carpenter* Court adopted the same considerations that the *Jones* concurrences, and particularly that of Justice Sotomayor, proposed: the intrusion was comprehensive, intimate, retrospective, and efficient. *Compare id.* at 309–13, 138 S.Ct. 2206, *with Jones*, 565 U.S. at 415–16, 132 S.Ct. 945 (Sotomayor, J., concurring) (discussing same qualities), *and id.* at 429–30, 132 S.Ct. 945 (Alito, J., concurring in judgment) (discussing efficiency).

Based on those considerations, the Court concluded that the CSLI intrusion violated the defendant's reasonable-privacy expectation. *Carpenter*, 585 U.S. at 313, 138 S.Ct. 2206. Then, in a separate section of the opinion, the *Carpenter* Court further distinguished *Smith* and *Miller* by explaining that the conveyance of CSLI is also not *voluntary*. *Id.* at 313–16, 138 S.Ct. 2206.

Leading scholars agree that *Carpenter* created a factor-based test derived from those considerations, though they disagree on which factors are the most important or mandatory. *E.g.*, Paul Ohm, *The Many Revolutions of* Carpenter, 32 Harv. J.L. & Tech. 357, 363, 369 (2019) (recognizing *Carpenter* created "new, multi-factor test" to analyze an individual's reasonable privacy expectation against intruding technology and

"herald[ed] a new mode of Constitutional analysis"); Susan Freiwald & Stephen W. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 Harv. L. Rev. 205, 219 (2018) (multifactor analysis was "clearly central" to the Court's holding); Tokson, *The Aftermath of* Carpenter, *supra*, at 1830 (describing the "*Carpenter* factors" and concluding from a survey of cases that "[a] multifactor *Carpenter* test has begun to emerge from the lower court[s]"). In reaching this conclusion, scholars rely on the Court's analysis and its concluding sentence, which reads: "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Carpenter*, 585 U.S. at 320, 138 S.Ct. 2206. In my view, such a factor-based examination is the correct interpretation of the Court's opinion.

Again, central to the Court's analysis was one overarching principle: the need to maintain historical Fourth Amendment protections against expanding police surveillance capabilities. Throughout its analysis, *Carpenter* extensively emphasized that the government historically could not conduct intrusions as *comprehensive*, *retrospective*, *intimate*, and *efficient* as those made possible by technological advancements like CSLI. *See, e.g.*, *id.* at 304–05, 138 S.Ct. 2206 (stating the Fourth Amendment analysis with respect to digital data must be "informed by historical understandings" of reasonable searches (quotations omitted)); *id.* at 305, 138 S.Ct. 2206 (discussing historical expectations); *id.* at 312, 138 S.Ct. 2206 (retrospective information was traditionally "unknowable"); *id.* at 320, 138 S.Ct. 2206

(stating that the police's use of CSLI infringed upon the Framers' intent in enacting the Fourth Amendment).

This rationale reflects the Court's understanding that rapid technological advances have created shifts "in kind and not merely in degree from the technology of the past." *Ohm*, *supra*, at 399. These shifts required the Court to adjust its analysis of the Fourth Amendment to "preserv[e the] degree of privacy ... that existed when the Fourth Amendment was adopted," as it has with technological changes in the past. *Carpenter*, 585 U.S. at 305, 138 S.Ct. 2206 (quoting *Kyllo*, 533 U.S. at 34, 121 S.Ct. 2038); *see id.* at 305–06, 138 S.Ct. 2206 (describing this philosophy in the Court's Fourth Amendment jurisprudence and citing cases); *id.* at 318, 138 S.Ct. 2206 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."); *see also* Orin S. Kerr, *The Digital Fourth Amendment: Implementing* Carpenter 10, 16–19 (USC Law Legal Studies Paper No. 18-29) (describing this phenomenon in the Court's jurisprudence as an "equilibrium-adjustment"); Denae Kassotis, *The Fourth Amendment and Technological Exceptionalism After* Carpenter: *A Case Study on Hash-Value Matching*, 29 Fordham Intell. Prop. Media & Ent. L.J. 1243, 1302 (2019) (explaining that *Riley* and *Carpenter* reflect the Court's understanding of the exceptional nature of technology and adaptation of the law to protect privacy).

Put simply, the Court declined to extend existing doctrines to exempt CSLI from Fourth Amendment protections based on the principle that it first recognized decades earlier: previously unimaginable technology

that reveals unprecedented amounts of personal information requires new rules. *Carpenter*, 585 U.S. at 310–14, 138 S.Ct. 2206 (citing the *Jones* concurrences and rejecting the "mechanical" application of old doctrines); *accord Riley*, 573 U.S. at 393, 134 S.Ct. 2473 (stating that comparing a physical search to a cell phone search is like "saying a ride on horseback is materially indistinguishable from a flight to the moon"). Thus, "[t]he beating heart" of *Carpenter* "is its deep and abiding belief in the exceptional nature of the modern technological era." Ohm, *supra*, at 399.

To sum up, the Court concluded that "personal location information maintained by a third party" lies at the intersection of the public-surveillance and third-party cases, but that neither theory "neatly" applies. *Carpenter*, 585 U.S. at 306, 138 S.Ct. 2206. Because the nature of such data is "unique," "an entirely different species," "qualitatively different," and represents a "seismic shift[ ]" in technology, the Court squarely declined to apply the third-party doctrine to it. *Id.* at 309, 313, 318, 138 S.Ct. 2206. Instead, the Court adopted a new test: it identified four qualities (comprehensiveness, retrospectivity, intimacy, and ease of access) that render CSLI fundamentally different from the records that police could traditionally obtain without a warrant, and it also noted that the act of sharing CSLI with the third-party wireless company departed drastically from that of sharing older forms of records. And because of those fundamental differences, the Court held that the defendant maintained a reasonable expectation of privacy in his CSLI records, notwithstanding that they were shared with a third party.

To that end, the Court also employed a normative analysis of each factor. That analysis did not rest solely on the facts of the intrusion in that specific case nor assess society's empirical expectations of privacy. Rather, the Court focused on the inherent nature of the data collected, its potential as technology advances, and whether such capabilities *should* be constrained by the Fourth Amendment. *E.g.*, *id.* at 313, 138 S.Ct. 2206 (in analyzing comprehensiveness, disregarding the actual precision of the CSLI intrusion at bar and stating that "the rule the Court adopts must take account of more sophisticated systems that are already in use or in development" (cleaned up)); *see also id.* at 311, 138 S.Ct. 2206 (concluding that CSLI revealed intimate information, without assessing what information the data actually revealed about the defendant); *Ohm*, supra, at 386 (explaining that *Carpenter* adopted a normative analysis of each factor that focused on the capabilities of CSLI as a category of information).

Consequently, a faithful application of *Carpenter* requires lower courts to adapt traditional Fourth Amendment principles to safeguard historical constitutional rights against steadily infringing technologies. To be sure, *Carpenter* provided factors that are relevant to that analysis without resolving which of those factors are mandatory and which should enjoy greater weight. But the Court clearly considered the factors in their totality, with an eye toward maintaining historical expectations of privacy.

II.

A.

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. That conclusion is evident upon evaluating how the *Carpenter* factors apply to the Location History intrusion in this case.

1.

The first factor that *Carpenter* identified was the comprehensiveness of the intrusion, focusing on CSLI's near-perfect surveillance capabilities. *Carpenter*, 585 U.S. at 311–12, 138 S.Ct. 2206. The Court looked at this factor from two dimensions: the depth and the breadth of the intrusion.

Regarding depth, the data collected in this case and in *Carpenter* was extremely comprehensive, involving a deep intrusion into each user's privacy rights. But the intrusion into Chatrie's Location History was even more comprehensive than the intrusion in *Carpenter* because Location History is collected more often and is more precise than CSLI as described in *Carpenter*.

In *Carpenter*, the Court was concerned that CSLI provided "near perfect surveillance" of its owner and created a "detailed, encyclopedic, and effortlessly compiled" record. *Id.* at 309, 138 S.Ct. 2206. The *Carpenter* Court concluded that the CSLI intrusion provided nearly perfect surveillance because, unlike police tracking of a vehicle—which a person exits and

which remains parked outside—a cell phone remains permanently attached to its owner and "faithfully follows" them into private areas. *Id.* at 311–12, 138 S.Ct. 2206 ("A cell phone—almost a 'feature of human anatomy'—tracks nearly exactly the movements of its owner." (citation omitted) (quoting *Riley*, 573 U.S. at 385, 134 S.Ct. 2473)); *see id.* at 311, 138 S.Ct. 2206 (noting many people even use their cell phones in the shower).

So too here. As with CSLI, Location History tracks a smartphone's location, so it likewise provides "near perfect surveillance" of its user. *Id.* at 311–12, 138 S.Ct. 2206. And like CSLI, Location History is collected with sufficient frequency to be able to faithfully track the user's movements.

Location History, however, provides even more detailed surveillance than CSLI because it is collected much more often. In *Carpenter*, CSLI only captured Carpenter's location when he affirmatively placed or received a call—no call, no data. *Id.* at 302, 138 S.Ct. 2206. But the Court also recognized that in recent years, companies had begun collecting CSLI from other "routine data connections." *Id.* at 301, 138 S.Ct. 2206. In line with its normative approach, the Court considered those advancements in its analysis, stating that with CSLI, the suspect has "effectively been tailed every moment of every day for" as long as the company maintained its records (in that case, five years). *Id.* at 312, 138 S.Ct. 2206.

While the "every moment" description was not accurate to Carpenter's own CSLI data—and was likely at least a slight exaggeration even considering the advancements

in CSLI technology by the time of the *Carpenter* decision[3]—it *does* essentially capture what we know of Location History data because that technology *automatically tracks users every two minutes*. *United States v. Chatrie*, 590 F. Supp. 3d 901, 908 (E.D. Va. 2022). So with Location History, police can reconstruct a user's movements with startling precision. The numbers in this case bear this out: through Location History, the police were able to collect an average of about 76 data points on each person surveilled *in just two hours*. Compare that to CSLI, which collected only about 101 data points on Carpenter *in a full day*. *Carpenter*, 585 U.S. at 302, 138 S.Ct. 2206. Thus, Location History data is even more "detailed, encyclopedic, and effortlessly compiled" than CSLI. *Id.* at 309, 138 S.Ct. 2206.

Additionally, Location History implicates even deeper privacy concerns than the CSLI in *Carpenter* because not only does it collect far more data points about each user, but also it is markedly more *precise*. In *Carpenter*, the data placed the defendant within a "wedge-shaped sector," *id.* at 312, 138 S.Ct. 2206, that ranged from "a dozen" to "several hundred" city blocks and was "up to 40 times more imprecise" in rural areas, *id.* at 324, 138 S.Ct. 2206 (Kennedy, J., dissenting) (noting CSLI is even less precise than GPS).

---

[3] According to *Carpenter*, "[w]hile carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections." *Carpenter*, 585 U.S. at 301, 138 S.Ct. 2206. The opinion does not clarify how frequently the collection of data from "routine data connections" occurs.

Here, by contrast, the district court found that "Location History appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing location data." *Chatrie*, 590 F. Supp. 3d at 907. In fact, Location History can hunt down a user's whereabouts within *meters*, and even discern elevation, locating the specific *floor in a building* where a person might be. *Id.* at 908–09.

Most critically, it is a fundamental legal principle that any intrusion into a constitutionally protected space receives Fourth Amendment protection. *E.g.*, *Karo*, 468 U.S. at 714–15, 104 S.Ct. 3296 (search occurred where government monitored a beeper inside "a private residence, a location not open to visual surveillance"); *Kyllo*, 533 U.S. at 33–35, 121 S.Ct. 2038 (search occurred where government used device to monitor radiation through home's walls). And Location History data is so granular that it can pinpoint and continuously follow a device inside protected spaces. For example, the geofence in this case covered over 17 acres and encompassed a nearby church. *Chatrie*, 590 F. Supp. 3d at 918. The district court found that the geofence could have also captured a hotel, "several units of [an] apartment complex," "a senior living facility," and "what appear to be several residences" for one hour at Step One, and it had *no* geographic limits for an additional hour in Step Two.[4] *Id.* at 923. It appears nearly

[4] As a reminder, Step One of the geofence warrant "'compel[led] Google to disclose a de-identified list of all Google users' whose Location History data indicates were within the geofence during a specified timeframe." *Chatrie*, 590 F. Supp. 3d at 914–15 (cleaned up). At Step Two, law enforcement could compel Google to provide

impossible to limit geofences to public spaces because Location History can inaccurately sweep more ground than police requested, [5] and Google does not set geographic limits on Step Two in standard geofence warrants. *Id.* at 916, 922–23.

Consequently, every geofence in a developed area could potentially reveal information "that could not otherwise have been obtained without physical intrusion into a constitutionally protected area." *Kyllo*, 533 U.S. at 34, 121 S.Ct. 2038 (internal quotation marks omitted); *see, e.g.*, Jake Snow, *Cops Blanketed San Francisco In Geofence Warrants. Google Was Right to Protect People's Privacy*, ACLU of N. Cal. (Jan. 7, 2024), https://www.aclunc.org/blog/cops-blanketed-san-francisco-geofence-warrants-google-was-right-protect-peoples-privacy [https://perma.cc/2Y7S-DRBG] (analyzing all geofence warrants from January 2018 to August 2021 in

---

additional location information for a narrowed list of users "*beyond* the time and geographic scope of the original request." *Id.* at 916. Google "imposes no geographical limits on this Step 2 data." *Id.* (quotation marks omitted).

Additionally, Google has no "firm policy as to precisely *when* a Step 2 request [has] sufficiently narrow[ed]" the list of users captured in Step One for whom police could request more data at Step Two. *Id.*

[5] While Location History is more precise than CSLI, it is not infallible. The district court found that the "largest confidence interval" for a user located within the geofence had a radius of roughly 387 meters—more than twice as large as the geofence. *Chatrie*, 590 F. Supp. 3d at 922–23. Thus, the court found that the "Geofence Warrant *could* have captured the location of someone who was hundreds of feet outside the geofence." *Id.* at 922. The court found that the government did not craft the geofence to account for these inaccuracies. *Id.* at 930–31.

San Francisco and finding that—in that area alone—the geofences covered hundreds of residences, twelve places of worship, seven medical sites of care, and other private spaces). That crosses a "bright" line: police need a warrant. *Kyllo*, 533 U.S. at 40, 121 S.Ct. 2038.

The majority opinion dismisses this concern, concluding that even though the instant geofence intrusion did surreptitiously enter several constitutionally protected spaces—including residences—this issue must be saved for future cases because the intrusion did not actually enter Chatrie's home, and he therefore lacks Fourth Amendment standing to challenge it on that ground.[6] Maj. Op. at 330 n.17, 336–37, 337 n.26. But that analysis is incorrect. The rules are simple: a person has Fourth Amendment standing if they have a reasonable expectation of privacy in the thing searched. Whether a person has a reasonable expectation of privacy in certain data is *inextricable from the data's capabilities*.

Citizens have a fundamental privacy expectation in non-public spaces, particularly their homes. *E.g.*, *Kyllo*, 533 U.S. at 34, 121 S.Ct. 2038; *Karo*, 468 U.S. at 714–15, 104 S.Ct. 3296. Accordingly, all citizens would reasonably expect privacy in data that continuously and retrospectively tracked their movements in these protected spaces with remarkable precision, even locating the specific room they occupy within a secure area.

---

[6] I note that it is unclear from the record whether the geofence intrusion indeed reached inside Chatrie's home or his constitutionally protected spaces.

It follows then that Chatrie would have a reasonable expectation of privacy from such an intrusion that could capture a church and residences at Step One and was boundless at Step Two. *Chatrie*, 590 F. Supp. 3d at 914–16. Indeed, police executed a search that *would* have captured Chatrie's home or other constitutionally protected space if it was in the Step One boundary, or if he happened to travel there during Step Two. It does not matter that Chatrie *happened* to stay outside of constitutionally protected spaces during a search that would have otherwise captured those spaces. *See Arizona v. Hicks*, 480 U.S. 321, 325, 107 S.Ct. 1149, 94 L.Ed.2d 347 (1987) ("A search is a search, even if it happens to disclose nothing but the bottom of a turntable.").

The *Kyllo* majority rejected the similar argument that the search of heat waves emanating from the home did not implicate the Fourth Amendment if the search did not catch more intimate information. That argument, Justice Scalia explained, was not only "wrong in principle," but also "impractical" because "no police officer would be able to know in advance" whether his surveillance will "pick[ ] up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." *Kyllo*, 533 U.S. at 38–39, 121 S.Ct. 2038. Likewise, here, when police executed an intrusion that would capture private spaces, they had no crystal ball to predict whether Chatrie would enter those spaces during the intrusion.

It was also the case in *Carpenter* that no facts showed that the CSLI intrusion entered the defendant's own protected spaces. But that did not affect his standing.

The Court simply held that because the CSLI intrusion had the capability to follow the defendant into any of numerous sorts of sensitive spaces, the intrusion was unlawfully intimate. *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206 ("A cell phone faithfully follows its owner *beyond public thoroughfares* and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." (emphasis added)). That is, the Court focused on the surveillance tool's *capabilities* during the intrusion as opposed to the specific facts of each intrusion. Because an intrusion into two days' worth of Carpenter's CSLI data met the *Carpenter* factors, Carpenter had a reasonable privacy expectation in that data and thus had standing. In so holding, the *Carpenter* Court affirmatively instructed lower courts to consider the potential reach of each intrusion, without regard to whether the intrusion indeed invaded the defendant's own private space under traditional Fourth Amendment standing principles. *Id.* The government thus cannot circumvent the Constitution merely because, by sheer luck, its target did not stray from the safe zone.

In short, the intrusion into Chatrie's Location History satisfies the depth portion of *Carpenter*'s first factor because it provides nearly perfect surveillance of its owner and creates a "detailed, encyclopedic, and effortlessly compiled" record of the owner's movements. *Id.* at 309, 138 S.Ct. 2206. And the intrusion was so broad that it did in fact enter private areas. This factor weighs strongly in favor of holding that the police conducted a Fourth Amendment search.

2.

Next is the intrusion's breadth (the second part of factor 1), which should be considered alongside its retrospective capabilities (factor 2) because the two are related.

Regarding breadth, the *Carpenter* Court was particularly concerned that wireless companies retained CSLI data for five years and stored that information for millions of people. This consideration was intertwined with the retrospective quality of the data: that is, because the wireless companies retained CSLI data for five years, police could "reconstruct a person's [past] movements," such that the person "has effectively been tailed every moment of every day for five years." *Id.* at 312, 138 S.Ct. 2206; *see id.* at 313, 138 S.Ct. 2206 ("[S]eismic shifts in digital technology ... made possible the tracking of not only Carpenter's location but also everyone else's ... for *years and years*." (emphasis added)); *id.* at 315, 138 S.Ct. 2206 (same).

This breadth deviated from historical privacy expectations, leading the Court to conclude the data was therefore qualitatively different from data the Court had previously concluded did not implicate the Fourth Amendment. *Carpenter* highlighted that police historically could not "reconstruct a person's [past] movements" without facing "a dearth of records and the frailties of recollection." *Id.* at 312, 138 S.Ct. 2206. But with CSLI, police could "travel back in time to retrace a person's whereabouts" with precision, not only in the recent past, but going back years. *Id.* Not only that, but CSLI data was also available for "400 million devices in

the United States"—not just those of suspects—so "this newfound tracking capacity runs against everyone." *Id.* Unlike with the trackers in *Knotts* or *Jones*, "police need not even know in advance whether they want to follow a particular individual [using CSLI], or when." *Id.*

Location History raises the same breadth and retrospectivity concerns: at the time of the geofence intrusion at issue here, Google collected and retained Location History records from the time Location History was enabled, which could have taken place years prior. This means that the data obtained in a geofence intrusion is pulled from a preexisting database of users' past movements, empowering police to time travel for each intrusion. Thus, each user has "effectively been tailed" since they activated Location History. *Id.*; *see also Chatrie*, 590 F. Supp. 3d at 909. Plus, like CSLI, Location History data is available for "numerous tens of millions" of unsuspecting Google users. *Chatrie*, 590 F. Supp. 3d at 907.

Yet, geofence intrusions are even broader than the intrusion in *Carpenter* because there is *no* limit on the number of users police can include in a geofence. With CSLI, police at least had to provide a specific phone number to search, so they had to identify a criminal suspect before they could pry into his or her historical CSLI data. By stark contrast, geofence intrusions permit police to rummage through the historical data of an unlimited number of individuals, *none* of whom the police previously identified nor suspected of any wrongdoing. Indeed, the very *point* of the geofence intrusion is to identify persons whose existence was unknown to police before the search.

Geofence intrusions are accordingly low-value fishing expeditions. So, even when police *do* obtain a warrant for a geofence, such a warrant is uncomfortably akin to the sort of "reviled" general warrants used by English authorities that the Framers intended the Fourth Amendment to forbid. *Carpenter*, 585 U.S. at 303, 138 S.Ct. 2206 (quoting *Riley*, 573 U.S. at 403, 134 S.Ct. 2473) (describing roots of the Fourth Amendment); *see also Steagald v. United States*, 451 U.S. 204, 220, 101 S.Ct. 1642, 68 L.Ed.2d 38 (1981) ("The general warrant specified only an offense ... and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." (citations omitted)). Now that the majority has eliminated the warrant requirement in cases like this one, police do not even need to "specif[y] ... an offense" before they can conduct a geofence intrusion. *Id.*

It follows that the breadth portion of the first factor (comprehensiveness) and the second factor (retrospectivity) weigh in favor of concluding that the geofence intrusion in this case was a search under *Carpenter*.

3.

Turning to the third factor, intimacy, *Carpenter* concluded that because CSLI captured "near perfect surveillance," it uncovered information that was personally revealing and thus intimate. *Carpenter*, 585 U.S. at 312, 138 S.Ct. 2206. As a result, this factor also favored the conclusion that the Fourth Amendment

applied. *Id.* at 311–12, 138 S.Ct. 2206. The same is true here.

Just like CSLI, Location History provides near-perfect surveillance, enabling the government to reconstruct a "detailed and comprehensive record of [Chatrie's] movements" for two hours. *Id.* at 309, 138 S.Ct. 2206. The government could learn a great deal about Chatrie in those two hours: the geofence intrusion occurred in "a busy part of the Richmond metro area" between 3:50 pm and 5:50 pm. *Chatrie*, 590 F. Supp. 3d at 919, 925. That is when most people leave work or school and travel to their next destinations, carrying their phones into intimate spaces and engagements. A two-hour search 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. *See* J.A. 145 (Google LLC's amicus brief filed in the district court, arguing that its users maintain a reasonable expectation of privacy in their Location History against a geofence intrusion, for there is "nothing limited" about a 2-hour geofence intrusion).

This is not a mere supposition. At the suppression hearing, Chatrie's defense counsel demonstrated that the identities of innocent users caught up in the geofence were easily deduced from the anonymized data that Google provided in Step 2. *Chatrie*, 590 F. Supp. 3d at 923–24. To make this showing, the defense took three users who were caught in the geofence—that is, innocent individuals who just happened to be near the site of the robbery—and demonstrated that the data the police

received from Google pursuant to its warrant retroactively tailed those individuals into private spaces: all three traveled to or from residences, one traveled to a school, and one traveled to a hospital. *Id.* at 923. Chatrie's expert also showed how deductions from this information allowed him to easily uncover those individuals' identities. *Id.* at 923–24.

And, as noted above, it does not matter whether the intrusion here revealed intimate information about Chatrie personally. *Carpenter* did not mention any facts that the CSLI search revealed about the defendant in that case—rather, the Court assessed only whether the search *could* reveal intimate information unrelated to legitimate police needs. *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206. The search here certainly could—and did.

Simply put, there can be no doubt that "[a]s with [the] GPS information" in *Jones*, or the CSLI in *Carpenter*, "the time-stamped data" from a geofence intrusion "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious and sexual associations.'" *Id.* at 311, 138 S.Ct. 2206 (quoting *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (Sotomayor, J., concurring)); *accord Smith*, 442 U.S. at 751, 99 S.Ct. 2577 (Marshall, J., dissenting) (recognizing that because people "value" privacy in basic activities, "the prospect of unregulated governmental monitoring [related to which phone numbers they dial] will undoubtedly prove disturbing even to those with nothing illicit to hide"). Additionally, because the geofence intrusion could enter constitutionally

protected spaces, it by default could reveal intimate information. *Kyllo*, 533 U.S. at 37, 121 S.Ct. 2038.

It is also of little importance that the intrusion here was of a shorter duration than in *Carpenter*. The government in *Carpenter* conducted two intrusions: it requested records of Carpenter's movements over both a seven- and 152-day period, which respectively revealed two and 127 days of data. *Carpenter*, 585 U.S. at 302, 138 S.Ct. 2206. The Court stated that the 127 days of data provided an "intimate window into a person's life" that revealed the litany of associations that Justice Sotomayor identified in her *Jones* concurrence. *Id.* at 311, 138 S.Ct. 2206 (citing *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (Sotomayor, J., concurring)). But the 127-day figure was nowhere near outcome-determinative: *Carpenter* ultimately held that only *two days* of CSLI data was intimate enough to constitute a search. *Id.* at 310 n.3, 138 S.Ct. 2206. Even the two-day figure is not dispositive because the Court expressly limited its holding to the facts before it, and thus did not address whether a shorter search would invoke constitutional scrutiny. *Id.* Moreover, the Court's intimacy analysis relied on Justice Sotomayor's concurrence in *Jones*, which argued that *short-term* searches are no less intimate by virtue of their limited duration. *See id.* at 311, 138 S.Ct. 2206 (citing *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (Sotomayor, J., concurring)).

Indeed, *Carpenter* only mentioned two temporal periods in the main text of the opinion—it stressed repeatedly that CSLI records and stores data for "years," *id.* at 312, 313, 315, 319, 138 S.Ct. 2206, and concluded that tracking over "127 days" creates a comprehensive record, *id.* at

311, 138 S.Ct. 2206—while holding in a footnote that the much shorter duration of *two days* of data collection still constituted a search, *id.* at 310 n.3, 138 S.Ct. 2206. So, the Court clearly focused on the character of the search, rather than its length. Location History operates the same way: like CSLI, Location History records and stores data for years, and it likewise provides nearly perfect, comprehensive surveillance. Thus, the fact that the intrusion here lasted only two hours does not preclude a finding that it revealed intimate information or constituted a search.

Finally, the majority opinion cites *Knotts* and this Court's en banc holding in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, in which this Court held that Baltimore's weeks-long aerial-surveillance program constituted a Fourth Amendment search. The majority relies on these cases for the principle that only prolonged tracking like that in *Beautiful Struggle*—as opposed to "short-term tracking of public movements" like in *Knotts*—implicates the Fourth Amendment. Maj. Op. at 334 (quoting *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021)). In the majority opinion's view, the geofence intrusion at bar is like the one-trip beeper intrusion in *Knotts*, and hence not a search. *Id.* at 330–31.

But the majority opinion's simplistic comparison to *Knotts* is inapt because it ignores the glaring differences between the beeper surveillance in *Knotts* and the vastly more sophisticated Location History technology here. Specifically, *Knotts* involved brief *real-time* public surveillance with a "rudimentary" technology that only

augmented officers' natural-born senses. *Carpenter*, 585 U.S. at 306, 138 S.Ct. 2206 (describing *Knotts*). By contrast, a geofence intrusion involves a retrospective (for years), continuous, nearly perfect surveillance technology, which enters private areas and captures information historically unavailable to uninvited human senses.

As elaborated on further below, *infra* at 368–70, *Knotts* and *Beautiful Struggle* involved the tracking of only *public* movements. Yet, as *Carpenter* held, intrusions into CSLI are categorically different from intrusions that only capture public movements. *See Carpenter*, 585 U.S. at 311–12, 138 S.Ct. 2206. For all the reasons I've explained, the same is true of the Location History data in this case. The geofence intrusion here was so broad that it could have followed users through dozens of non-public spaces, including residences, religious spaces, and senior living facilities. Thus, the intrusion did not merely constitute a "short-term tracking of *public* movements." *Beautiful Struggle*, 2 F.4th at 341 (emphasis added).

In sum, Location History can reveal intimate information about an individual, so the third *Carpenter* factor favors a finding that police obtaining Location History data must obtain a warrant.

4.

The fourth *Carpenter* factor, ease of access, also favors this conclusion. Geofences, like CSLI searches, are "easy, cheap, and efficient compared to traditional investigative tools." *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206. As with CSLI, police conduct a geofence intrusion

"[w]ith just the click of a button" that enables them to scour the continuous locations of numerous people in any area at any time—"at practically no expense." *Id.*; *see also* Ohm, *supra*, at 369 (noting that cell phone location tracking is almost twice as cheap as GPS tracking, while GPS tracking is 28 times cheaper for police than covert pursuits). In fact, geofence intrusions are remarkably "easy" because Google does most of the work *for* the police.

In considering this factor, *Carpenter* heeded the concerns raised in the *Jones* concurrences, which cautioned against enabling powerful leaps in police surveillance capabilities through practical advances. *See Jones*, 565 U.S. at 429–30, 132 S.Ct. 945 (Alito, J., concurring in the judgment) ("In the precomputer age, the greatest protections of privacy were ... practical."); *id.* at 416, 132 S.Ct. 945 (Sotomayor, J., concurring) (warning that government abuse would ensue from the unrestrained police power to use advanced and efficient, relatively low-cost technology). In his *Jones* concurrence, Justice Alito emphasized that if a digital search would have been exceptionally demanding and costly for police to replicate in the pre-digital age, then society does not reasonably expect that search to occur. *Id.* at 429–30, 132 S.Ct. 945 (Alito, J., concurring in the judgment). A geofence intrusion certainly would have been impossible to replicate in the pre-internet age. So, it violates society's privacy expectations.

The fourth factor therefore favors the conclusion that police engage in a search when they obtain geofence data.

5.

The final factor to consider is voluntariness. To be sure, it is unclear whether *Carpenter* requires us to consider voluntariness at all. That's because the Court expressly concluded that the defendant had a reasonable expectation of privacy in his CSLI records and that the third-party doctrine did not apply *before* it ever addressed voluntariness. *See Carpenter*, 585 U.S. at 313, 138 S.Ct. 2206. However, in its summation at the end of the opinion, the Court stated that "[i]n light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and *automatic nature of its collection*, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Id.* at 320, 138 S.Ct. 2206 (emphasis added). The reference to the "automatic nature of [the] collection" seemingly refers to voluntariness. This ambiguity is expected: *Carpenter* deliberately left open to interpretation the precise contours of its analysis. *See, e.g.*, Tokson, *The Aftermath of* Carpenter, *supra*, at 1798, 1800.

At minimum, the *Carpenter* Court's discussion of voluntariness in a separate rebuttal section—after the Court had already concluded the intrusion was a search—establishes that it is the least important factor in the overall analysis. *See* Matthew Tokson, *Smart Meters as a Catalyst for Privacy Law*, 72 Fla. L. Rev. F. 104, 112 (2022) ("Most scholars view involuntariness not as a requirement but as merely one factor among many examined in *Carpenter*. The Court's discussion of the voluntariness issue ... was mostly confined to a single

paragraph in a lengthy opinion that largely focused on [other] factors[.]" (footnote omitted) (collecting scholarship)); Freiwald & Smith, *supra*, at 219 (observing that *Carpenter* established a multiprong test made up of only the four primary factors already discussed).

Assuming arguendo that voluntariness is a mandatory factor to be considered in the analysis of whether a police intrusion into digital records constitutes a search, it is clear for reasons explained below that Chatrie's sharing of Location History was *not* meaningfully voluntary. Additionally, even if this factor slightly leans in the government's favor, this factor's contribution is marginal and insufficient to sway the balance of the factor-based test.

Carpenter rejected an extension of the third-party doctrine to CSLI intrusions, noting that CSLI differs from the records in *Smith* and *Miller* in part because the conveyance of CSLI is involuntary. *Carpenter*, 585 U.S. at 315, 138 S.Ct. 2206. That is, while *Smith* and *Miller* held that individuals had no reasonable privacy expectations in their bank records and phone numbers dialed because they voluntarily (and often physically) conveyed those records to third-party companies, *Carpenter* reasoned that individuals do not "voluntarily" convey their CSLI data to third parties merely by using their cell phones—at least not in any "meaningful sense." *Id.*

In so concluding, the Court reasoned that cell phones are a ubiquitous part of modern life. And the Court reasoned that individuals convey CSLI to wireless companies by

simply turning on their cell phones and connecting to the wireless network. After that, any cell phone activity generates CSLI.[7] *Id.* So, because cell phones are prevalent in modern society, and cell phone use necessarily creates CSLI without much action or awareness by the user, the Court concluded the conveyance of CSLI data is not "meaningful[ly]" voluntary. *Id.*

The sharing of Location History is likewise not "meaningful[ly]" voluntary. *Id.* First, like CSLI, once Location History is enabled, it is always generated and collected. In fact, Location History is even less voluntarily conveyed because it is conveyed automatically every two minutes, while CSLI is only conveyed when there is phone activity like an incoming text. And users are even less likely to be aware of the conveyance of Location History than they are CSLI because once users enable Location History, it is automatically conveyed *across all devices* on which a user is logged into Google, even when the user has deleted the Google app through which they opted into Location History. Thus, the ongoing conveyance of

---

[7] Again, the government in *Carpenter* only collected the defendant's CSLI data at the start and end of calls, and wireless companies likewise had long only collected CSLI data in those increments. *Carpenter*, 585 U.S. at 301, 302, 138 S.Ct. 2206. But the Court recognized that "in recent years," companies had also begun collecting CSLI from the transmission of text messages and routine data connections. *Id.* at 301, 138 S.Ct. 2206. Although those advancements did not apply to Carpenter himself, the Court considered them in its analysis of voluntariness.

Location History is more automatic and less voluntary than CSLI.

Compare that to the conveyances in *Smith* and *Miller*, in which individuals were much more aware that they were conveying information to third parties. In *Smith*, the individuals physically dialed each number they conveyed, and the phone company sent monthly bills listing some of the calls that the companies had collected. *Smith*, 442 U.S. at 742, 99 S.Ct. 2577 (noting users "see a list of their long-distance (toll) calls on their monthly bills"). And of course, in *Miller*, individuals had to physically convey checks and deposit slips to the bank. *Miller*, 425 U.S. at 442, 96 S.Ct. 1619; *e.g.*, Alyssa Bentz, *First in Online Banking*, Wells Fargo History (last visited Apr. 1, 2024), https://history.wf.com/first-in-online-banking/ [https://perma.cc/FRT2-XHRR] (noting that in 1984—eight years after *Miller* was decided—internet banking software had not been developed so customers "still had to input their [bank] transactions by hand"). The nature of such a physical conveyance differs drastically from a cell phone's automatic conveyance every two minutes.

Second, a substantial number of individuals generate Location History, just like CSLI. To be sure, Google's Location History service tracks fewer Americans than does CSLI. *Compare Chatrie*, 590 F. Supp. 3d at 907 (Google did not provide specific numbers but revealed it tracks "numerous tens of millions" of users), *with Carpenter*, 585 U.S. at 300, 138 S.Ct. 2206 (noting that "[t]here are 396 million cell phone service accounts in the United States," which is greater than the number of people). And the majority contends that the fact "[t]hat

two-thirds of active Google users have not enabled Location History is strong evidence" that opting in is voluntary. Maj. Op. at 331.

But the use of technology is not per se voluntary just because the adoption of that technology is not as ubiquitous as the cell phone. Tens of millions of citizens opt into using technologies like 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 those technologies record the most intimate, retrospective information about them. *See, e.g.*, William Gallagher, *Apple Watch Sets New US Record, now Owned by 30% of iPhone Users*, Apple Insider (Oct. 14, 2022), https://appleinsider.com/articles/22/10/14/apple-watch-sets-new-us-record-now-owned-by-30-of-iphone-users [https://perma.cc/DJ2P-LR7B] (100 million active users of Apple Watch in 2022); *Flo Health Inc. Company Update, March 2022*, Flo Health (Mar. 16, 2022), https://flo.health/newsroom/flo-company-update [https://perma.cc/N7Q6-V3UF] (220 million downloads of popular menstrual-cycle app); Krystal Hu, *ChatGPT sets record for fastest-growing user base - analyst note*, Reuters (Feb. 2, 2023), https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/ [https://perma.cc/R63F-EAPC] (100 million monthly users of ChatGPT within two months of launching).

Google alone has 1.5 billion users worldwide. *See* NYU Technology Law & Policy Clinic Amicus Brief at 5 n.4. Even if only one-third opt into Location History, that is a whopping 500 million people, many of whom are Americans. And millions more opt into substantially

identical location tracking through other technologies.[8] Far be it from me to tell hundreds of millions of Americans that they have waived their privacy rights with the State just because these invasive technologies are not fully automatic or because not *every single* user utilizes them.

Third, the gloss of an opt-in checkbox does not render the enabling of Location History collection "meaningful[ly]" voluntary.[9] *Carpenter*, 585 U.S. at 315,

---

[8] While Location History is Google-specific, millions of Americans use substantially similar technologies offered by other companies. In *Carpenter*, the Court referred to the *total* number of cell phone service accounts in the United States, as opposed to the number of accounts with the specific wireless company that the defendant used. *Carpenter*, 585 U.S. at 300, 302, 138 S.Ct. 2206. Thus, the correct analysis in assessing whether a technology is widely adopted and hence "indispensable to participation in modern society," *id.* at 315, 138 S.Ct. 2206 (quotation omitted), is to consider the total number of users of substantially similar technologies.

[9] According to the majority, a user must (1) enable location sharing on their device; (2) enable the "Location Reporting" feature; (3) sign into Google; and (4) opt into the Location History setting. But the district court made no mention of, nor any findings of fact regarding, the enabling of location sharing or Location Reporting (the majority's requirements 1 and 2). *See Chatrie*, 590 F. Supp. 3d at 907–12. Rather, the district court concluded that users enable the Location History feature solely by opting into Location History and logging into their Google accounts.

Even if all four steps were required to enable Location History, the record indicates that these steps may be accomplished in the first few moments of setting up and using an Android device. Chatrie used a standard Android cell phone with Google's operating system. That type of phone comes out of the box with the location-sharing setting enabled *by default*, thus automatically satisfying requirement (1). Next, the record indicates that by enabling

138 S.Ct. 2206. This one click does not meaningfully inform users that they are surrendering "a comprehensive dossier of [their] physical movements." *Id.*

Instead, the pop-up text that appears when Google prompts users to opt in explains only that Location History "[s]aves where you go with your devices," and that "[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com." *Chatrie*, 590 F. Supp. 3d at 911–12. Below that, the screen provides the options: "NO, THANKS" or a brightly highlighted "TURN ON." *Id.* at 912. It also presents a small expansion arrow, which, if tapped by the user, displays more information about Location

---

Location History, users can also automatically opt-in to Location Reporting. So, requirements (2) and (4) are not necessarily two separate steps; they can be completed with one click.

Likewise, one of the first steps in setting up an Android is to log into or create a Google account. Indeed, if users choose not to log into Google, they cannot use most of the Android's features such as downloading apps, music, and games; accessing Google Maps; or syncing services like Calendar and Contacts. The district court found that Google repeatedly prompts its millions of Android users to opt-in to Location History both upon initial set-up and then "multiple times across multiple apps." *Id.* at 908–09 (cleaned up). For example, "Google may prompt the user to enable Location History first in Google Maps, then *again* when he or she opens Google Photos and Google Assistant for the first time." *Id.* at 909 (emphasis added). Thus, requirement (3) is also satisfied quickly and without reference to Location History.

History.[10] But a user does not need to click the expansion arrow to opt into Location History. They can just click "TURN ON." Through that click, Location History is enabled.

The district court noted that this pop-up "did not detail ... how frequently Google would record [a user's] location ...; the amount of data Location History collects (essentially all location information); that even if he 'stopped' location tracking it was only 'paused' ... ; or, how precise Location History can be (i.e., down to twenty or so meters)." *Id.* at 936 (cleaned up). Nor did it inform users that Google would automatically and precisely track their location even when they were not doing anything on their phones, or that this tracking would occur across all devices on which they were logged in—not just those on which they opted in—even when they have deleted the respective Google app. *Id.* at 909–12 (quoting terms); *see id.* at 909 n.11, 913–14 & n.16 (discussing wide criticism of Google because its Location History opt-in and opt-out procedures were unclear to users); *cf. Jones*, 565 U.S. at 417 n.*, 132 S.Ct. 945 (Sotomayor, J., concurring) ("[S]mart phone[ ] [owners] do not contemplate that these devices will be used to enable covert surveillance of their movements.").

---

[10] The expansion arrow reveals the following additional information: "Location History saves where you go with your devices. To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, like Google Maps or Search.... This data may be saved and used in any Google service where you were signed in to give you more personalized experiences." *Chatrie*, 590 F. Supp. 3d at 912.

I agree with the district court's conclusion that the warnings provided by Google are "limited and partially hidden" and that it is "plain that these 'descriptive texts' are less than pellucid." *Chatrie*, 590 F. Supp. 3d at 936. Simply put, the pop-up box lacked sufficient information for users to knowingly opt into Location History. Smartphone users are bombarded with opt-in buttons and terms of service in their daily phone use. Few actually read the terms, and, without reasonably clear descriptions, most users do not understand what they are approving. *See Jones*, 565 U.S. at 417, 132 S.Ct. 945 (Sotomayor, J., concurring) (pointing out that Americans are revealing intimate information during "mundane" tasks); *Research Shows Mobile Phone Users Do Not Understand What Data They Might Be Sharing*, Sci. Daily (May 9, 2023), https://www.sciencedaily.com/releases/2023/05/230509122057.htm [https://perma.cc/54V5-Y49P] (discussing study that showed a substantial portion of users do not understand how phone and app tracking works).

Further, while the majority opinion argues that users can delete information, *see* Maj. Op. at 330–31, that is easier said than done. To delete their Location History, a user has "only one option": they must visit the proper website, locate their timeline, and delete their data. *Chatrie*, 590 F. Supp. 3d at 913. And the deletion of past Location History data will not turn off the collection of *additional* Location History data. As the district court indicated, the process of enabling, pausing, and deleting Location History is *not* transparent to users. *See id.* at 913–14, 936; *see also id.* at 913 (finding that Google falsely told users that pausing Location History will limit the functionality of Google services).

For instance, the district court quoted an internal email by a Google staffer who expressed their frustration that the Location History interface is "difficult enough that people won't figure ... out" how to turn off the feature. *Id.* at 913. The district court determined that the sentiment in that email is "certainly not inconsistent with the record before the Court." *Id.* What's more, around the time Chatrie enabled the feature, Google faced criticism from members of Congress, the media, and Norway's Consumer Protection Committee for the lack of transparency in how users enable or disable Location History. *See id.* at 909 n.11; *id.* at 913–14; *id.* at 913 n.16.[11]

The explosive growth of the usage of new technologies, such as smartphones, illustrates a certain level of comfort among the American populace in entrusting personal information to technology companies like Google. But that does not mean such trust extends to the State or that the American populace has ceded its reasonable expectation of privacy in that information.

---

[11] The majority opinion argues that the evidence is "nonexistent" that pausing or deleting Location History is easier said than done. Maj. Op. at 339 n.30. But the majority provides no evidence of its own that pausing and deleting Location History is a reasonable process for users, beyond stating conclusively that users can figure it out. *Id.* at 330–31, 339 n.30. And to the contrary, criticism from the news media, congressional members, a consumer-protection group, and Google staffers themselves regarding the difficulty of pausing or deleting Location History certainly constitutes evidence of the same. Moreover, though the district court did not conduct fact-finding on this issue, it did conclude that such criticisms appeared consistent with the record and that Google's warnings were "less than pellucid." *Chatrie*, 590 F. Supp. 3d at 936, 913.

Americans might expect that companies provided with their information will, at most, barrage them with advertisements. The State, by contrast, holds a monopoly on licit violence and detainment. It is a grave misjudgment to conflate an individual's limited disclosure to Google with an open invitation to the State. *See Jones*, 565 U.S. at 418, 132 S.Ct. 945 (Sotomayor, J., concurring) ("I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."); *Smith*, 442 U.S. at 749, 99 S.Ct. 2577 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").

As noted, *Carpenter* endorses a normative understanding of modern technology and with it a normative understanding of voluntariness. *See Carpenter*, 585 U.S. at 315, 138 S.Ct. 2206 (concluding that "*in no meaningful sense* does the [cell phone] user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements" (emphasis added) (cleaned up)). Although bank records and the dialing of phone numbers are similarly central to participation in modern society, the Court in *Carpenter* opted to treat the conveyance of CSLI as uniquely involuntary. This demonstrates a recognition that modern technology, particularly that which tracks an individual's location, warrants heightened privacy requirements.

In sum, even if voluntariness might be considered as a factor in the *Carpenter* test, the conveyance of Location History data to third parties is not meaningfully voluntary. And even assuming arguendo that it is marginally more voluntary than the conveyance of CSLI was in *Carpenter*, the balance of the *Carpenter* factors nonetheless strongly supports the conclusion that the geofence intrusion constituted a search.

* * *

Because the balance of the *Carpenter* factors shows that Location History is qualitatively different from the records that police could traditionally obtain without a warrant, Chatrie had a reasonable expectation of privacy in his Location History data, and the government conducted a search by accessing it. In the context of this novel technology, the third-party doctrine is wholly inadequate to defeat that reasonable expectation. While geofence intrusions may be a boon to law enforcement, they still require a warrant.

B.

My friends in the majority rest their contrary holding on Section III(B) of *Carpenter*, in which the Court rebutted the government's insistence that *Smith* and *Miller* should resolve the case. In so doing, the majority decision holds that the proper analysis under *Carpenter* is a direct analogy to the third-party doctrine established by *Smith* and *Miller*. *See* Maj. Op. at 332 ("The third-party doctrine ... squarely governs this case.").

But *Carpenter* affirmatively *rejected* a "straightforward application" of *Smith* and *Miller*, establishing that analogizing the third-party cases to "qualitatively different" records like CSLI and Location History is misguided. *Carpenter*, 585 U.S. at 309, 314, 138 S.Ct. 2206; *see id.* at 314, 138 S.Ct. 2206 ("The Government ... is not asking for a straightforward application of the third-party doctrine, but instead *a significant extension of it* to a distinct category of information.... In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI." (emphasis added)); *see also id.* at 313, 138 S.Ct. 2206 (rejecting Government's argument that "cell-site records are fair game because they are 'business records' created and maintained by the wireless carriers").

Thus, *Smith* and *Miller* do not control here because the *Carpenter* Court rejected a simplistic analogy to those cases when dealing with advanced digital surveillance. Further, even if such an analogy were proper, the nature of the records collected here is incomparable to those in third-party cases like *Smith* and *Miller* so the application of the third-party doctrine fails. Indeed, the third-party doctrine has two requirements: first, the nature of the documents sought by police must be unrevealing business records like those in *Smith* and *Miller*, and second, the conveyance to the third-party company must be meaningfully voluntary. As *Carpenter* emphasized, "*Smith* and *Miller* ... did not rely solely on the act of sharing. Instead, [those decisions] considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of

privacy" concerning their contents.'" *Id.* at 314, 138 S.Ct. 2206 (quoting *Miller*, 425 U.S. at 442, 96 S.Ct. 1619). So even if the conveyance of Location History was voluntary, the *Carpenter* Court repeatedly stressed that the nature of location data derived from a smart phone—such as the CSLI data in *Carpenter*, or the Location History data here—is simply incomparable to that sought in *Smith* and *Miller*.

In analyzing the "nature of the particular documents sought" in this case, the majority decision instead concludes that the geofence intrusion here was "far less revealing than that obtained in *Jones*, *Carpenter*, or *Beautiful Struggle* and more like the short-term public movements in *Knotts*." Maj. Op. at 330–31.

But that's an improper comparison. Instead, the proper comparison in applying the *third-party doctrine* would be to the bank documents and pen register in the *third-party cases*, *Smith* and *Miller*—not to the public-surveillance cases cited in the majority decision. *E.g.*, *Carpenter*, 585 U.S. at 313–14, 138 S.Ct. 2206 (comparing CSLI to the documents in *Smith* and *Miller*); *id.* at 306, 138 S.Ct. 2206 (distinguishing public surveillance and third-party doctrine cases); *Smith*, 442 U.S. at 741–43, 99 S.Ct. 2577 (addressing nature of records); *Miller*, 425 U.S. at 440–43, 96 S.Ct. 1619 (same). The majority opinion's failure to grapple with *Smith* and *Miller*, while insisting that "[t]he third-party doctrine ... squarely governs this case," Maj. Op. at 332, is telling.

As discussed above, the *Carpenter* Court took great pains to emphasize that the nature of technology like CSLI is "unique," "an entirely different species," "a

qualitatively different category" of information, and data that represents a "seismic shift[ ]" in technology as compared to the phone numbers dialed and bank records in *Smith* and *Miller*. *Carpenter*, 585 U.S. at 309, 313, 318, 138 S.Ct. 2206. And as my analysis has shown, the first four *Carpenter* factors demonstrate that the "nature" of Location History, like CSLI, differs by orders of magnitude from the records at issue in the third-party cases.

Beyond that, *Carpenter* rejected the application of the third-party doctrine by explaining that the third-party cases relied on the unrevealing nature of the documents sought. *Id.* at 313–14, 138 S.Ct. 2206. For instance, *Carpenter* explained, the *Smith* Court stressed that the phone numbers lacked any content or "identifying information" in holding there was no reasonable expectation of privacy. *Id.* at 314, 138 S.Ct. 2206 (cleaned up); *see also Smith*, 442 U.S. at 741, 99 S.Ct. 2577.

By contrast, Location History, like the CSLI in *Carpenter*, reveals that information. Thus, "[s]uch a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Carpenter*, 585 U.S. at 315, 138 S.Ct. 2206. *Carpenter* emphasized that unless courts recognize this difference, they will "fail[ ] to appreciate that there are no comparable limitations on the revealing nature of CSLI." *Id.* at 314, 138 S.Ct. 2206. So too here. *Carpenter* hence rejected the view that the nature of personal-location data matches that of traditional bank or phone records, urging courts to consider the context of *Smith* and *Miller*'s analyses.

Thus, even if the conveyance of Location History was voluntary, the first prong of the third-party-doctrine test—the nature of the records conveyed—is nowhere near satisfied and the application of the doctrine here fails. Accordingly, *Carpenter* compels the conclusion that the police intrusion into Chatrie's Location History data constituted a Fourth Amendment search.[12]

III.

Before concluding, I respond to what the majority opinion structures as a lengthy separate opinion that responds to my dissent, Maj. Op. at 332–39.

Extrajudicially, the majority's separate opinion claims that *Carpenter*'s factor-based test was "concocted" from thin air. *Id.* at 333. Instead, the majority opinion believes that (1) *Carpenter* should be read narrowly to apply only the "established" privacy principles pronounced in *Jones*, *id.* at 333–34; (2) employing a factor-based test would "abandon[ ]" all pre-*Carpenter* case law, *id.* at 332–33, 336–37; and (3) despite the *Carpenter* Court's

---

[12] The government did obtain a warrant in this case. But I agree with the lower court that the warrant here was so lacking in particularity and probable cause that it was invalid. *Chatrie*, 590 F. Supp. 3d at 927. And the good-faith exception to the warrant requirement does not apply because the warrant lacked any indicia of probable cause. The government's proposed justification—that the robber used a cell phone and a cell phone *could* have Google Location History turned on—is extremely broad. Also, the government did not limit the scope of the warrant to an area reasonably related to the bank robbery. Accordingly, a reasonable officer could not have relied on the warrant in good faith. I would thus grant Chatrie's Motion to Suppress the evidence that resulted from the geofence search.

warnings about applying old tests to new technologies, the third-party doctrine can nonetheless definitively settle this case, *id.* at 332–33, 336–37. All three beliefs are unsound.

A. *Carpenter* Established a Multifactor Analysis

In an attempt to restructure the Supreme Court's holding in *Carpenter*, the majority folds that decision into *Jones*, saying that *Jones* had established certain rules regarding the privacy implications of digital technology and first identified the relevant factors, and that *Carpenter* merely applied those rules and factors. *See id.* at 333 (claiming that *Carpenter* simply "appl[ied] the principles announced in the location-tracking cases"); *id.* at 333–34 (asserting that *Jones* considered unique qualities of GPS technology like that it is "detailed, encyclopedic, and effortlessly compiled," and *Carpenter* merely "applied" those "established principles" to CSLI). So, with that, the majority declares that *Carpenter* accomplished nothing new.

But that's wrong. As we acknowledged in *Beautiful Struggle*, *Jones* "was ultimately decided on trespass principles." *Beautiful Struggle*, 2 F.4th at 341. Indeed, the *Jones* majority analyzed only the trespass doctrine, expressly declining to consider the privacy implications of a GPS intrusion under *Katz*. *Jones*, 565 U.S. at 406–07, 132 S.Ct. 945. Significantly, it was the *concurring justices* in *Jones* who pointed out the unique attributes of GPS technology and argued that the *Katz* reasonable-expectation-of-privacy test could have decided the case.

Specifically, in his concurring opinion, Justice Alito, joined by three other Justices, argued that the long-term GPS intrusion in *Jones* violated *Katz* because society did not historically expect police to conduct such prolonged surveillance on public streets due to practical limitations like cost. *Id.* at 429–30, 132 S.Ct. 945 (Alito, J., concurring in judgment). And it was Justice Sotomayor who, writing alone, discussed several unique attributes of GPS—that it is precise, comprehensive, intimate, retrospective, and cheap—and argued that those attributes implicate the *Katz* analysis for even short-term GPS surveillance. *Id.* at 415–16, 132 S.Ct. 945 (Sotomayor, J., concurring). So, it was the concurrences in *Jones*—and particularly that of Justice Sotomayor, writing alone—that recognized the unprecedented power of modern location-tracking technology and argued for the need to adjust Fourth Amendment protections to maintain traditional privacy expectations against such technologies. But, prior to *Carpenter*, that view was not binding precedent.

Carpenter hence broke new ground: it placed the principles proposed in the *Jones* concurrences (the four-justice opinion of Justice Alito coupled with the concurring opinion of Justice Sotomayor) into a majority opinion and articulated how location data obtained from a cell phone is different from traditional modes of surveillance. As explained, the *Carpenter* majority derived most of its factor-based test from Justice Sotomayor's lone concurrence in *Jones*. In addition, *Carpenter* marked the first time that the Court in a majority opinion recognized a privacy interest in the "whole of [a person's] physical movements," and it weighed those factors to analyze that interest.

Carpenter, 585 U.S. at 310, 138 S.Ct. 2206. So, *Carpenter* marked a new era of Fourth Amendment jurisprudence even as it built on the cases that came before it, setting forth how we must think about the Fourth Amendment in the context of modern technology.

Thus, the majority opinion's claim that *Carpenter* merely "applied established principles" is wrong. Maj. Op. at 334. And to confirm that, we need to look no further than the *Carpenter* opinion itself, which explicitly stated that its decision "d[id] not fit neatly under existing precedents." *Carpenter*, 585 U.S. at 306, 138 S.Ct. 2206. That statement alone should end this discussion but in the interest of completeness, I will respectfully address the remainder of the majority opinion's complaints about *Carpenter*'s multifactor analysis.

The majority opinion scoffs that the factor-based test does not exist. Maj. Op. at 332–34. But this dissent's analysis of the test comes directly from *Carpenter*'s text, in which the Supreme Court took great pains to make clear that the third-party doctrine cannot extend to novel technologies like CSLI that have the qualities the Court identified. The Court's efforts were apparently in vain, however, because the majority opinion continues to "mechanically apply[ ] the third-party doctrine" in defiance of the Supreme Court's repeated and express commands not to do so. *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206.

Remarkably, while alleging that this dissenting opinion's analysis lacks any basis in *Carpenter*, the majority opinion simultaneously complains that this

dissent quotes *Carpenter too much*—particularly the Court's language stressing the distinct nature of CSLI and directing courts to move away from past doctrine when analyzing such technology. *See* Maj. Op. at 333 & n.21. That's just poppycock. Instead of engaging with the substance of the Supreme Court's quoted language that forms most of *Carpenter*'s analysis, the majority answers by essentially saying we should ignore that language.

Still further, the majority opinion posits that the "'factors' identified by [this] dissent ... were not factors at all" but were instead "attributes" of CSLI that "implicated the privacy interest recognized by the concurring Justices in *Jones*." *Id.* at 333. That is a distinction without a difference. In other words, although the majority quibbles about how to characterize the Court's analysis (factors vs. attributes), it recognizes that those factors (or attributes) are derived directly from *Carpenter*'s text. For example, the majority agrees that the CSLI in *Carpenter* implicated the reasonable-expectation-of-privacy test because the CSLI had "immense capabilities": that is, it "provided a '*comprehensive* record' of [the defendant's] movements, which revealed *intimate* details of his life .... And the *retrospective* nature of CSLI and the *ease* by which it could be accessed only augmented these privacy concerns, for no comparable record of a person's movements was available to law enforcement in a pre-digital age." *Id.* (emphases added) (quoting *Carpenter*, 585 U.S. at 309, 138 S.Ct. 2206). Because CSLI had each of those qualities, the majority opinion concedes, "CSLI warranted Fourth Amendment protection." *Id.*

In so conceding, the majority opinion applies the exact factors I recognize in this dissent, pointing out that, post-*Carpenter*, we consider comprehensiveness, intimacy, retrospectivity, and ease when determining whether a digital intrusion violates the Fourth Amendment. So, whether we call the qualities that we weigh "attributes" or "factors" is immaterial. As explained, *supra* at 345–46, the *Carpenter* Court did not expressly state that it created a factor-based test; it identified the qualities of CSLI that informed its holding. The legal community—including three of the dissenting Justices on the *Carpenter* Court, *see Carpenter*, 585 U.S. at 340, 138 S.Ct. 2206 (Kennedy, J., joined by Thomas and Alito, JJ., dissenting)—has concluded that those qualities created a factor-based test.

So the factor-based test is certainly not the "creative[ ]" project of this dissenting opinion, as the majority suggests. Maj. Op. at 335 n.27; *accord id.* at 333 (characterizing this dissent's "pronouncements" as "bold" and its "framework" as "novel"); *id.* (criticizing this dissent for "combin[ing] ... ingredients" from *Carpenter* to "create[ ] a new inquiry from scratch" in order to—"*voila!*"—find that a search occurred); *id.* at 339 (arguing that this dissent's test is "novel" and "unwieldy"). Instead, it represents the scholarly consensus that *Carpenter* diverged from existing precedent and created a new, multifactor analysis. In addition to the leading authorities this dissenting opinion has already cited, *see supra* at 346–47 (first citing Ohm, *supra*, at 363, 369; then citing Freiwald & Smith, *supra*, at 219; and then citing *Tokson*, *The Aftermath of* Carpenter, *supra*, at 1830), numerous other scholars and

authorities to have considered the issue have concluded the same, *see*, *e.g.*, Sherwin Nam, *Bend and Snap: Adding Flexibility to the* Carpenter *Inquiry*, 54 Colum. J.L. & Soc. Probs. 131, 132 (2020) (stating that *Carpenter* "broke new ground in the constitutional right to privacy in electronic data" and employed a "five-factor" test); Helen Winters, *An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants*, 107 Minn. L. Rev. 1369, 1381, 1390 (2023) (stating *Carpenter* "marked a new period of Fourth Amendment jurisprudence" and described "several factors relevant to its decision"); Antony Barone Kolenc, *"23 and Plea": Limiting Police Use of Genealogy Sites After* Carpenter v. United States, 122 W. Va. L. Rev. 53, 71–72 (2019) (concluding that *Carpenter* "alter[ed] Fourth Amendment law" by recognizing a privacy interest in the "whole of a person's physical movements," and "balanced five factors" to analyze that interest); Allie Schiele, *Learning from Leaders: Using* Carpenter *to Prohibit Law Enforcement Use of Mass Aerial Surveillance*, 91 Geo. Wash. L. Rev. Arguendo 14, 17–18 (2023) (pointing out "*Carpenter*'s focus on five central factors"); Nicole Mo, *If Wheels Could Talk: Fourth Amendment Protections Against Police Access to Automobile Data*, 98 N.Y.U. L. Rev. 2232, 2251 (2023) (recognizing factors); Luiza M. Leão, *A Unified Theory of Knowing Exposure: Reconciling* Katz *and* Carpenter, 97 N.Y.U. L. Rev. 1669, 1684 (2022) (same); Matthew E. Cavanaugh, *Somebody's Tracking Me: Applying Use Restrictions to Facial Recognition Tracking*, 105 Minn. L. Rev. 2443, 2468 (2021) (same).

Finally, the majority opinion laments that the multifactor analysis only works if *Carpenter* created a

test "from scratch." *Id.* at 333. But that is far from the case.

Rather, *Carpenter* articulated the factors as a way to analyze whether an individual has a reasonable privacy expectation in their digital location data. So, the Court applied the long-standing *Katz* standard, but it adapted the *Katz* analysis for digital data like CSLI to preserve privacy protections against encroaching technologies—which, as *Carpenter* explained, the Court has done throughout its Fourth Amendment jurisprudence. *Carpenter*, 585 U.S. at 304–05, 138 S.Ct. 2206 (noting that the Court "ha[s] kept ... Founding-era understandings [of privacy] in mind when applying the Fourth Amendment to innovations in surveillance tools" and citing cases in which the Court "rejected ... a 'mechanical interpretation' of the Fourth Amendment" for novel surveillance tools (citations omitted)).

Thus, *Carpenter*'s analysis *began* by providing this context and explaining the Court's enduring understanding that expansive technologies require heightened protections. *Id.* at 304–05, 138 S.Ct. 2206. In so doing, the Court situated the remainder of its analysis within that context. And the Court repeated those sentiments throughout the opinion. The majority opinion ignores these critical aspects of *Carpenter*.

Carpenter also acknowledged the Court's existing third-party-doctrine precedent but explained that the *Carpenter* factors render the "nature" of CSLI markedly different from the nature of the documents in the third-party cases. *Id.* at 308–10, 138 S.Ct. 2206. In addition, the Court's opinion incorporated ideas about

technology and privacy from past cases like *Kyllo*, *Riley*, and the *Jones* concurrences. *E.g.*, *id.* at 310–13, 138 S.Ct. 2206. For these reasons, *Carpenter*'s multifactor analysis was "informed" by case law and adapted for a new era. *Id.* at 305, 138 S.Ct. 2206.

But not to be deterred even in a world ever transfigured by technology, the majority opinion apparently wants to scold the *Carpenter* Court for stepping beyond the shadows of *Knotts*, *Smith*, and *Miller* when faced with surveillance technology that is not only different in degree, but different in kind. I must disagree, because the Supreme Court's analysis in *Carpenter* aptly reflects the traditional evolution of law. That is, the Supreme Court wisely moved beyond its decades-old precedent to reiterate that it is not required to robotically copy and paste precedent when dealing with novel issues arising from changing technology.

Nonetheless, the majority opinion contends that the Supreme Court could not have possibly "abandoned" *Knotts*, *Jones*, *Smith*, and *Miller* in the face of new technology. Maj. Op. at 332–33, 336-37. I agree that the Supreme Court did no such thing. That's because *Jones* was resolved under trespass principles; *Knotts* involved surveillance of a suspect during one trip on public roads using what *Carpenter* called a "rudimentary" beeper, *Carpenter*, 585 U.S. at 306, 138 S.Ct. 2206; and *Smith* and *Miller* involved police obtaining bank records and dialed phone numbers, which *Carpenter* emphasized were "a world" apart from data like CSLI and Location History, *id.* at 314, 138 S.Ct. 2206.

Thus, *Carpenter* did not "abandon" *Knotts*, *Smith*, and *Miller*—instead, it explained that they do not neatly apply to technologies like CSLI and Location History. In so holding, *Carpenter* acknowledged a simple truth: the digital age does not strip us of our Constitutional protections.

And this principle is not what the majority calls a radical departure because it is no more revolutionary than the novel acknowledgments in *Katz* that the "Fourth Amendment protects people, not places," or in *Riley* that our cell phones are not merely external attachments, but intimate extensions of our private lives. *Id.* at 304–05, 138 S.Ct. 2206 (first quoting *Katz*, 389 U.S. at 351, 88 S.Ct. 507; and then citing *Riley*, 573 U.S. at 393, 134 S.Ct. 2473). At bottom, *Carpenter* binds this Court and we must follow it.

B. The *Complete* Third-Party Analysis, Intimacy, and Standing

The majority opinion also complains that the Location History intrusion at bar did not reveal information as intimate as that in *Carpenter* and *Beautiful Struggle*, and that the use of Location History is voluntary. Maj. Op. at 334–39. Relatedly, the majority opinion reiterates that even if the intrusion entered private spaces, Chatrie lacked Fourth Amendment standing to challenge it because, as far as we know, it did not enter *his* protected spaces.

In other words, the majority opinion emphasizes two of *Carpenter*'s five factors (intimacy and voluntariness)—but it ignores the remaining three factors

(comprehensiveness, in terms of both depth and breadth; retrospectivity; and efficiency), likely because they weigh indisputably in Chatrie's favor. It likewise ignores the other prong of the third-party doctrine, the nature of the documents sought, which similarly forecloses the use of that doctrine. I address the third-party doctrine before discussing intimacy.

1.

First, take the third-party doctrine. As the majority makes clear, it believes that the use of Location History is meaningfully voluntary because the average user should know from Google's popups, which the district court called "limited and partially hidden" and "less than pellucid," that Google will infinitely track the user's Location History data. *Chatrie*, 590 F. Supp. 3d at 936. But nothing in the majority opinion's lengthy response to my dissent addresses the first requirement of the third-party doctrine—the nature of the documents collected. The third-party doctrine has *two* requirements. First, the "nature of the particular documents sought" must be akin to the unrevealing business records (the phone numbers dialed and bank records) at issue in *Smith* and *Miller*. *Carpenter*, 585 U.S. at 314, 138 S.Ct. 2206 (quoting *Miller*, 425 U.S. at 442, 96 S.Ct. 1619). Second, those records must be voluntarily conveyed to the third-party business. *Id.*

As discussed above, the majority opinion's third-party-doctrine analysis is flawed because it wrongly compares the "nature of the documents" at issue here to the nature of the surveillance in *Knotts* (outdoor beeper surveillance), *Jones* (outdoor GPS-tracker surveillance),

and *Beautiful Struggle* (outdoor aerial surveillance), even though those cases did not involve the conveyance of records to third parties. Rather, to properly apply the *third-party doctrine*, we must compare the nature of the documents in this case to those in the *third-party doctrine* cases, i.e., *Smith* and *Miller*. By instead selecting inapt comparators, the majority opinion crafts a Frankensteinian analysis that lacks a basis in precedent or logic. And while it insists that the third-party doctrine "squarely" applies here, Maj. Op. at 331–32, the majority opinion ignores comparisons to the documents in the third-party doctrine's seminal cases.

As *Carpenter* stressed, the nature of CSLI and Location History data today is miles apart from that of phone and bank records in the 1980s. Because the first prong of the third-party doctrine fails, so too does the application of the doctrine to this case. So, a straightforward application of the doctrine mandates the conclusion that a Fourth Amendment search occurred here.

2.

The majority opinion next relies on *Beautiful Struggle*, in which this Court held that Baltimore's weeks-long public aerial surveillance constituted a Fourth Amendment search, to conclude that the two-hour intrusion at bar could not gather data that was sufficiently intimate so as to implicate the Fourth Amendment. Thus, the majority opinion argues that, unlike the longer intrusion in *Beautiful Struggle*, the intrusion here was too short to reveal intimate information and thus was not a search. Maj. Op. at 334–36. In so arguing, the majority opinion expounds on its

assertion that Chatrie lacked standing to challenge the intrusion if it did not enter his private spaces. *Id.* at 336–37. These arguments relate to the majority opinion's final objection that *Beautiful Struggle* did not recognize any factor-based inquiry from *Carpenter*, and thus, the majority opinion reasons, one does not exist. *Id.* at 333–34.

These arguments fall flat. As I explain, the intimacy discussion in *Beautiful Struggle* does not foreclose a finding of intimacy here because that case involved technology that was only capable of surveillance of public movements. And the majority opinion misrepresents that *Beautiful Struggle* did not recognize any factor-based test from *Carpenter* because that opinion expressly applied the *Carpenter* factors.

As a threshold matter, however, the majority opinion's argument is unclear. It claims that *Carpenter* did not apply any multifactor analysis, and that *Beautiful Struggle* instead established its own test: a search occurs when police "use technology to monitor [an individual's] long-term movements, but not when they glimpse only his short-term movements." *Id.* at 334. In other words, the majority opinion remarkably proposes that the Fourth Amendment only considers whether an intrusion using modern technology was long or short. But then the majority opinion informs us that "Location History has capabilities much like GPS data and CSLI," *id.* at 335, seemingly referring to the *Carpenter* factors, which should be irrelevant to the supposedly sole question of an intrusion's length. And, as noted, in another portion of its response to my dissent, the majority opinion tellingly applies the *Carpenter* factors itself. *Id.* at 333–

34. In essence, the majority opinion flip-flops to reach a desired outcome. I nonetheless respond to its arguments.

a.

The majority opinion's argument that *Beautiful Struggle* forecloses a finding of intimacy for all relatively short intrusions misconstrues the opinion and stretches it further than the opinion can bear. To explain why *Beautiful Struggle* is not on point, I begin with some background.

In *Beautiful Struggle*, the Court considered Baltimore's aerial-surveillance program, which monitored only public spaces and stored that data for forty-five days. The aerial surveillance generally gathered hours-long chunks of surveillance during the day, and only showed individuals as anonymous, blurry pixels. *Beautiful Struggle*, 2 F.4th at 334, 340. As a result, the government had to decipher individuals' identities from several pieces of captured data. *Id.* at 334.

The key distinction between Baltimore's program and CSLI or Location History is that it strictly captured *public* movements. The Supreme Court has long held that individuals have a diminished privacy expectation in public spaces. *See Katz*, 389 U.S. at 351, 88 S.Ct. 507. As part of this diminished privacy expectation, the Court recognized in *Knotts* that beeper surveillance of one public trip did not implicate the Fourth Amendment. *Knotts*, 460 U.S. at 285, 103 S.Ct. 1081. Crucial to the *Knotts* Court's holding, however, was the beeper's rudimentary capabilities that merely augmented human senses, such that the surveillance mirrored that of a

passerby watching the defendant on the street. *See Carpenter*, 585 U.S. at 306–07, 138 S.Ct. 2206.

So, in analyzing the public surveillance in *Beautiful Struggle*, this Court had to begin with the tenet that one has a diminished privacy expectation in public, then to ask whether the surveillance was so invasive as to breach that diminished privacy expectation. And, if the intrusion was to be considered a Fourth Amendment search, it would have to be more invasive than that in *Knotts*. This is where the duration of the intrusion becomes relevant. The district court in *Beautiful Struggle* had determined that Baltimore's aerial intrusion was not a search because the program captured only chunks of *public* movements. *Leaders of A Beautiful Struggle v. Balt. Police Dep't*, 456 F. Supp. 3d 699, 713–14 (D. Md. 2020) (reasoning that the intrusion could not reveal details inside of private spaces).

But this Court reversed, holding that the forty-five-day length of the public aerial surveillance implicated the *Carpenter* factors. That is, we held that because the government gathered chunks of public aerial footage daily for weeks, the cumulative data was "detailed, encyclopedic," "intimate," and "retrospective," and broadly comprehensive because it "recorded *everyone's* movements." *Beautiful Struggle*, 2 F.4th at 341–42 (cleaned up); *see id.* at 345 (explaining that people reasonably expect to be seen for a short period in public, but they do not expect longer public intrusions). And we emphasized that the weeks-long duration of the intrusion permitted deductions by police that revealed "intimate" information about those surveilled. *Id.* at 342. For all those reasons, we determined that Baltimore's

relatively lengthy public surveillance "transcends mere augmentation of ordinary police capabilities" and hence triggered Fourth Amendment protections. *Id.* at 345.

So, while this Court in *Beautiful Struggle* did distinguish between a short-and long-term search, that was because the search at issue in that case covered strictly public areas. *Id.* at 341. Contrary to the majority opinion's assertions, the distinction that we drew in *Beautiful Struggle* regarding the length of the search was rooted in the factors that *Carpenter* identified. Its solely public sweep notwithstanding, the longer aerial intrusion was a search *because* it satisfied the *Carpenter* factors and thus violated the surveilled individuals' reasonable privacy expectations. *Id.* at 341–42, 346 (applying factors and concluding the intrusion was a search). If in *Beautiful Struggle* we believed those factors were irrelevant, as the majority opinion now presses, then we would have simply distinguished *Knotts* without saying more.

Technology that allows only for augmented public surveillance, however, is fundamentally different from technology that has the capacity to surveil private spaces, like CSLI and Location History.[13] This is nothing new: the Supreme Court has long drawn a line between public and private spaces—concluding that

---

[13] The majority opinion claims that we cannot even consider the differences in the capacities of the technologies at issue in *Beautiful Struggle* and the present case because the Location History data here only captured public movements. Maj. Op. at 336–37. But, as explained above, whether a person has a reasonable expectation of privacy in certain forms of data depends on the *capabilities* of that data. *Supra*, at 350–52.

using a beeper to track a vehicle for one trip on a public road is not a search, but monitoring a device within a constitutionally protected space is subject to Fourth Amendment constraints, even if the monitoring was brief or revealed nothing of value. *Compare Karo*, 468 U.S. at 714–15, 104 S.Ct. 3296, *with Kyllo*, 533 U.S. at 34, 121 S.Ct. 2038. Unlike in public, individuals do not have a diminished privacy expectation in private spaces. Accordingly, where a police intrusion can enter private spaces, the short-versus-long-term distinction holds much less weight.

Relatedly, the fact that Location History can perfectly surveil private spaces implicates one's reasonable privacy expectation because it exceeds historical expectations of police capabilities. In *Beautiful Struggle*, the Court reasoned that a short aerial intrusion only augmented what police could traditionally capture by tailing suspects. Only public surveillance for a longer duration amounted to "attaching an ankle monitor" to those surveilled, *Beautiful Struggle*, 2 F.4th at 341 (cleaned up), capturing information that police traditionally could not gather "without technology," *id.* So there, only the longer intrusion violated privacy expectations and became a search. But here, even two hours of a boundless Location History intrusion is akin to "attaching an ankle monitor" on the surveilled, capturing information inside private spaces that were historically closed to prying police eyes. That intrusion thus exceeds mere augmentation of human capabilities and becomes a search, even when the duration is short. *See id.* at 341, 343, 345 (emphasizing that the analysis turns on historical police capabilities).

Similarly, we also reasoned in *Beautiful Struggle* that it would take longer for police to deduce intimate information about individuals whom they only follow on discrete public trips like that in *Knotts*, meaning that the duration of surveillance in the public sphere is a key component of the intimacy factor. *Id.* at 342–43. But an intrusion that provides near-perfect surveillance in *private* spaces, like with Location History data, much more quickly reveals one's "familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (Sotomayor, J., concurring). So, again, the short-term and long-term distinction is less relevant outside of the public-surveillance context.

In sum, the majority opinion errs in contending that, following *Beautiful Struggle*, the only Fourth Amendment question before us is whether an intrusion was long or short. As our analysis in *Beautiful Struggle* demonstrated, we must ask whether an intrusion satisfied the *Carpenter* factors. While the length of the intrusion in *Beautiful Struggle* made clear that it did, a shorter intrusion into nonpublic spaces could satisfy the *Carpenter* factors as well—as it did here.

Next, the majority opinion argues that the geofence intrusion did not reveal intimate information because the two-hour window could have only revealed innocuous activities in private spaces, as opposed to scandalous or particularly sensitive activities. Maj. Op. at 335–36. It acknowledges that the geofence indeed could have captured users "seeing a friend for coffee, touring a housing upgrade, ... buying a couch off of Facebook marketplace," or inquiring into medical

services. *Id.* at 335. But because such innocuous activities would not reveal individuals' "habits, routines, and associations," the majority opinion argues, the intrusion was not sufficiently intimate to become a search. *Id.* at 335–36.

The majority opinion wrongly defines intimacy. *Beautiful Struggle* indeed held that surveillance that reveals one's "habits and patterns" is intimate. *Beautiful Struggle*, 2 F.4th at 343. But, contrary to the majority opinion's assertion, that is not the only information that is intimate for purposes of the Fourth Amendment reasonable-expectation-of-privacy test. Indeed, *Carpenter* made no mention of personal habits or patterns in its intimacy analysis. *Carpenter* instead held that an "intimate window" into a person's life is one that reveals "his 'familial, political, professional, religious, and sexual associations.'" *Carpenter*, 585 U.S. at 311, 138 S.Ct. 2206 (quoting *Jones*, 565 U.S. at 415, 132 S.Ct. 945 (Sotomayor, J., concurring)). The sheer breadth of that list of associations—which the Court held contains the sacred "privacies of life" in which one maintains a reasonable privacy expectation, *id.* (quoting *Riley*, 573 U.S. at 403, 134 S.Ct. 2473)—is telling. Of course, this Court's decision in *Beautiful Struggle* could not limit the reach of *Carpenter*; nor did it claim to do so. Instead, while habits and patterns relevant in *Beautiful Struggle* are indeed a *form* of intimacy, the litany of associations that *Carpenter* recognized are likewise intimate.

Because people have a reduced privacy expectation in public, it made sense that the public surveillance in *Beautiful Struggle* would only violate their privacy

expectation when the surveillance was so invasive that it permitted deductions about their "habits and patterns," from which police could decipher personal associations, which often manifest in non-public spaces. Habits and patterns are intimate precisely because they reveal the associations recognized in *Carpenter*. But when police can monitor individuals' precise movements in private spaces, the information revealed is much more intimate and likely to reveal one's familial, political, professional, religious, and sexual associations without the need for pattern-based deductions. Under the Fourth Amendment, Americans have a heightened privacy expectation from such intrusions.

The majority opinion's argument that innocuous information is not intimate is likewise unavailing. Two hours of innocuous activities in a busy urban area could certainly reveal the targets' associations. The Fourth Amendment has never incorporated a scandal barometer for information that constitutes the "privacies of life." *Id.* at 311, 138 S.Ct. 2206.

Simply put, the 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. This blanket rule has no basis in *Carpenter*, which expressly declined to address whether a specific duration was necessary to implicate Fourth Amendment protections. Nor could this blanket rule find a basis in *Beautiful Struggle*, which addressed only

police surveillance that captured blurry public movements.

b.

In the majority opinion's final attempt to argue that the intrusion here was not a search, the majority reiterates its argument that Chatrie had no standing to challenge the intrusion if it did not enter his own private spaces. *See* Maj. Op. at 330 n.17, 336–37, 337 n.26. Because the majority opinion merely repeats itself without engaging with my response, *supra* at 350–52, I will not rehash this issue.

Of note, the majority opinion focuses on intimacy and voluntariness in its lengthy response to this dissent. But intimacy is only one of the factors to which the Court looked in *Carpenter*. And even if the shorter duration of the intrusion in this case leads the intimacy factor to weigh less strongly in favor of deciding that the Fourth Amendment applies, it far from tips the scale given the immense weight of the comprehensiveness (in breadth and depth), efficiency, and retrospectivity of Location History. The majority opinion does not dispute that these factors apply to Location History.

As a self-provided example of "eviscerat[ing] basic and longstanding Fourth Amendment principles," Maj. Op. at 337 n.26, the majority opinion utterly fails to address the geofence's stark similarities to the reviled general warrants that the Fourth Amendment was intended to bar—similarities that will only increase given the majority opinion's elimination of the warrant requirement altogether. *See supra* at 352–53. At the very least, these historical similarities demand

heightened caution here, not the majority opinion's rigid application of the third-party doctrine.

3.

Our Supreme Court decided *Carpenter* on the principle that applications of the Fourth Amendment must evolve in step with technology to ensure that our constitutional protections are not rendered meaningless by new means of government intrusion. Rather than clinging to policy preferences for pre-*Carpenter* precedent, the Supreme Court in *Carpenter* directed courts to move past such basic analyses when considering unprecedented surveillance technology like CSLI.

It is our duty to apply *Carpenter* honestly and diligently. We should not and cannot sidestep the primary impact of a Supreme Court opinion to apply earlier decisions that are inapplicable, and simply put, more to our own liking. To do so would undercut *Carpenter* and thus, undermine our duty to faithfully guard Constitutional protections.

IV.

As a consequence of today's majority decision, significant concerns arise regarding the privacy rights of all Americans. That's why Justice Sotomayor's warning in *Jones* applies here with equal relevance—rejecting the warrant requirement for technology as cheap, readily accessible, and unprecedentedly powerful as a geofence intrusion is akin to inviting governmental abuse. *See Jones*, 565 U.S. at 416, 132 S.Ct. 945 (Sotomayor, J., concurring).

Ironically, court decisions like this one could also hinder legitimate law enforcement efforts. Shortly after oral arguments in this case, Google—apparently predicting the majority opinion's flawed reading of *Carpenter*—shut down the technology that permits geofence intrusions, [14] thereby reducing the potential for legitimate investigatory uses of this innovative technology, even with a warrant.

Another consequence of today's decision is that it could "alter the relationship between citizen and government in a way that is inimical to democratic society." *Jones*, 565 U.S. at 416, 132 S.Ct. 945 (Sotomayor, J., concurring) (cleaned up). This is because citizens may feel inhibited from exercising their associational and expressive freedoms, such as the right to peacefully protest and the ability of journalists to gather information confidentially and effectively, knowing "that the Government may be watching" them. *Id.*; *see* Reporters Committee for Freedom of the Press Amicus Brief at 7–8 (noting the CIA's track record of "follow[ing] newsmen ... in order to identify their sources" (citation omitted)); *Smith*, 442 U.S. at 751, 99 S.Ct. 2577 (Marshall, J., dissenting) ("The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide."); *see* NYU Technology Law & Policy Clinic Amicus Brief at 25 (noting that "[f]orced disclosure of membership can chill association, even if

---

[14] *E.g.*, Cyrus Farivar & Thomas Brewster, *Google Just Killed Warrants That Give Police Access to Location Data*, Forbes (Dec. 14, 2023), https://www.forbes.com/sites/cyrusfarivar/2023/12/14/google-just-killed-geofence-warrants-police-location-data/ [https://perma.cc/27JX-ANVC].

there is no disclosure to the general public"); *Ams. for Prosperity Found. v. Bonta*, 594 U.S. 595, 141 S. Ct. 2373, 2388, 210 L.Ed.2d 716 (2021) (holding that disclosure requirements risk chilling association). As a result of today's majority opinion, the government may 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. Without warrants, the government is free to surveil anyone exercising their First Amendment (or other) rights at the government's whim—using a technology that can identify each individual retrospectively, without any suspicion of criminal activity—and those surveilled will be none the wiser. All of that offends the Supreme Court's instruction that Fourth Amendment review must be particularly rigorous when First Amendment protections are at risk. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978).

* * *

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. New technologies that collect ever-more-intimate data are becoming integral to daily life in ways we could not have imagined even a short time ago. This fact of modern life—that we cannot know what developments, and what risks posed

by those developments, lie just around the corner—should counsel courts to exercise humility. The Supreme Court has guided us to safeguard against novel technologies that may enable government infringement on constitutional rights.

That's what we should do. At the end of the day, upholding the precious freedoms guaranteed by our Constitution is our duty. Because the majority decision fails to honor that duty today, I must, with great respect, dissent.

Appendix D

In The United States District Court,
Eastern District of Virginia
Richmond Division.

UNITED STATES of America

v.

Okello T. CHATRIE, Defendant.

Criminal Case No. 3:19cr130

Filed 03/03/2022

M. Hannah Lauck, United States District Judge

MEMORANDUM OPINION

I. Introduction

Ratified in 1791, the Fourth Amendment to the United States Constitution guarantees to the people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. To that end, the Framers prohibited the issuance of a warrant, unless that warrant was based "upon probable cause" and unless it "particularly describ[ed] the place to be searched, and the persons or things to be seized." *Id.* The Supreme Court of the United States has since applied the principles embodied in this language to constantly evolving technology—from recording devices in public telephone booths, *Katz v. United States*, 389 U.S. 347, 88

S.Ct. 507, 19 L.Ed.2d 576 (1967); to thermal-imaging equipment, *Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001); and, most recently, to cell-site location data, *Carpenter v. United States*, —— U.S. – ——, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018).

This case implicates the next phase in the courts' ongoing efforts to apply the tenets underlying the Fourth Amendment to previously unimaginable investigatory methods. In recent years, technology giant Google (and others) have begun collecting detailed swaths of location data from their users. Law enforcement has seized upon the opportunity presented by this informational stockpile, crafting "geofence" warrants that seek location data for every user within a particular area over a particular span of time. In the coming years, further case law will refine precisely whether and to what extent geofence warrants are permissible under the Fourth Amendment. In the instant case, although the Motion to Suppress must ultimately be denied, the Court concludes that this particular geofence warrant plainly violates the rights enshrined in that Amendment.

II. Findings of Fact and Procedural History

A. Findings of Fact[1]

1. The Robbery at the Call Federal Credit Union

On May 20, 2019, at approximately 4:52 p.m., a bank robbery occurred at the Call Federal Credit Union (the

[1] A "presumption of validity" exists "with respect to the affidavit supporting the search warrant." *Franks v. Delaware*, 438 U.S. 154,

"Bank") in Midlothian, Virginia. The suspect held a firearm over the course of the robbery and took $195,000 from the Bank.

During the robbery, the suspect presented a teller working at the Bank a handwritten note that stated:

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

(ECF No. 54-1, at 6.)[2] The teller told the suspect that she did not have access to that amount of money, and the

---

171, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978). Because Chatrie does not allege that the statements in the affidavits supporting the search warrants are untrue statements, but instead says that these statements do not provide enough information or that they do not contain the proper information to support the search warrants, the Court in part makes its findings of fact based on the statements made in the affidavits. *Id.* (describing the circumstances in which the Court must hold an evidentiary hearing on a defendant's motion to suppress).

[2] The Court employs the pagination assigned by the CM/ECF docketing system for citations to the parties' submissions. Where a document was not filed through CM/ECF (for example, an exhibit introduced at a hearing), the Court will cite to the pages that would

suspect then displayed a silver and black firearm. While openly holding the gun, the suspect directed the teller, other Bank employees, and the Bank customers to move to the center of the lobby and get on the floor. The suspect then led these individuals behind the teller counter to an area that contained the Bank's safe. Once behind the counter, the suspect forced the Bank's manager to open the safe and place $195,000 into a bag he brought with him. After acquiring the money, the suspect left the Bank on foot, "towards an adjacent business, west of the [B]ank." (ECF No. 54-1, at 6.)

During its investigation, law enforcement obtained the instant Geofence Warrant (hereinafter "Geofence Warrant" or "Warrant")—a novel application of search technology whose use has grown exponentially in recent years. Google produced certain location information pursuant to the Warrant, which led the police to Okello Chatrie. Chatrie was eventually charged with two

---

have been assigned through CM/ECF had they been filed through the system.

In addition, the Court acknowledges that its findings of fact differ between this Memorandum Opinion and a later issued Memorandum Opinion addressing the validity of four other warrants. In that Opinion, the warrants set forth a lengthier, more detailed narrative explaining the officers' investigatory steps than the instant Geofence Warrant. In determining the validity of a warrant, the "magistrate [or magistrate judge], and a reviewing court, will restrict their inquiries on probable cause to the facts set forth in the four corners of the officers' sworn affidavit." *United States v. Lipscomb*, 386 F. Supp. 3d 680, 684 (E.D. Va. 2019). Thus, because the facts in the Geofence Warrant differ from those set out in the four other warrants, the Court's findings of fact accordingly differ as well.

crimes related to the robbery.[3] He then filed a Motion to Suppress the Geofence Warrant that forms the basis of this Opinion.

2. The Record Presented to the Court by the Parties

There is a relative dearth of case law addressing geofence warrants.[4] In this case, the parties, especially the defense, pursued a thorough and deep record. This Court was aided by Amicus Google's provision of detailed information, including in-person testimony regarding the company's acquisition, retention, and use of users' location data. In what may be a first, Google filed an Amicus Brief.[5] Mr. Marlo McGriff, a Location

---

[3] More precisely, (1) Forced Accompaniment During Armed Credit Union Robbery, in violation of 18 U.S.C. §§ 2113(a), (d), and (e); and, (2) Using, Carrying, or Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A).

[4] Specifically, this Court has identified only five other federal opinions on the subject, but all assessed the validity of the warrants *before* they were issued: *In re Search of Information That is Stored at the Premises Controlled by Google LLC*, No. 21sc3217, 2021 WL 6196136 (D.D.C. Dec. 30, 2021); *In re Search of Information that is Stored at the Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153 (D. Kan. 2021); *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); and, *In re Search of Information Stored at Premises Controlled by Google*, No. 20M297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).

[5] Among other things, Google argued in its brief that Location History is not a business record, but is a journal stored primarily for the user's benefit and is controlled by the user. Google states that

History Manager at Google since 2016, submitted three declarations over the course of this matter. Ms. Sarah Rodriguez, a Team Lead for Legal Investigations Specialists ("LIS")[6] at Google since 2018, provided one declaration. During a hearing on March 4–5, 2021, (one of many in this case), the Court heard live testimony from both Mr. McGriff and Ms. Rodriguez.[7]

The parties to this case also brought their own experts. Spencer McInvaille, an expert in digital forensic examinations, forensics, and cellular location testified for the defense, and FBI Special Agent Jeremy D'Errico, a part of the cellular analysis survey team ("CAST") spoke for the Government. Multiple rounds of briefing occurred before, during, and after the hearings held by the Court.

In order to establish as thorough a record as possible with respect to this new technology, the Court will first

---

LH information "can often reveal a user's location and movements with a much higher degree of precision than [Cell Site Location Information]." (ECF No. 59-1, at 8.) Google argues that a geofence is certainly a "'search' within the meaning of the Fourth Amendment," because "[u]sers have a reasonable expectation of privacy in the LH information, which the government can use to retrospectively reconstruct a person's movements in granular detail." (ECF No. 59-1, at 9.)

[6] Legal Investigations Specialists are the Google employees who receive warrants and send the returns.

[7] This testimony was delayed at the request of defense counsel during an extensive period of time because the COVID pandemic prevented live testimony.

discuss Google's location services, as well as Google's typical response to geofence warrants.[8]

3. Google's Collection and Production of Location Data

a. Google's Suite of Location Services

Google collects detailed location data on "numerous tens of millions" of its users. (ECF No. 96-1, at ¶ 13; ECF No. 201, at 205.) It acquires and stores this data through one of at least three services: (1) Location History, (2) Web and App Activity ("WAA"), and (3) Google Location Accuracy ("GLA"). Google only searches Location History when it receives a geofence warrant.

i. Location History

Location History appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing *location* data. Google developed Location History to allow users to view their Location History data through its "Timeline" feature, a depiction of a user's collected Location History points over time. (ECF No. 96-1, at ¶ 5; *see* ECF No. 202, at 79.) According to Google, this permits Google account holders to "choose to keep track of locations they have visited while in possession" of their mobile device. (ECF No. 96-1, at ¶ 4.) Importantly, Location History also supports Google's advertising

---

[8] Other companies such as Amazon and Apple invariably retain users' location data as well. But Google, whose services function across Apple *and* Android devices (as opposed to Apple Maps for example, which functions only on iPhones), seems to be subject to more geofence requests than other companies.

revenue.[9] For instance, McGriff testified that Location History data serves Google's advertising business by providing "store visit conversions" or "ads measurement" to businesses based on user location. (ECF 201, at 196–97.) Without identifying any individual user, this "store conversion" data can follow a particular ad campaign and identify "how many users who saw a particular ad campaign actually went to one of those stores." (ECF No. 201, at 197.) Google's "radius targeting" also allows—again without identifying any user—"a business to target ads to users that are within a certain distance of that business." (ECF No. 201, at 198.)

Location History is powerful: it has the potential to draw from Global Positioning System ("GPS") information, Bluetooth beacons, cell phone location information from nearby cellular towers, Internet Protocol ("IP") address information, and the signal strength of nearby Wi-Fi networks. According to Agent D'Errico, Location History logs a device's location, on average, every two minutes.[10] Indeed, Location History even allows Google to "estimat[e] ... where a device is in terms of elevation."

---

[9] Using 10K filings from Google's parent company Alphabet, FBI Agent D'Errico noted that Google's advertising revenue constituted 85.4% and 83.9% of its *entire* revenue in 2018 and 2019, respectively.

[10] Defense Expert McInvaille evaluated a sample set of data and found that, for that data, Location History logged a device's location every six minutes. Under McInvaille's estimate, a user's movement is logged 240 times a day. D'Errico's estimate would raise that to 720 times a day. And Google Expert McGriff confirmed that Location History can track a user "hundreds" of times a day. (ECF No. 202, at 159.)

(ECF No. 202, at 95.) McGriff testified that this capability helps locate someone in an emergency, or try to "determine if you are on the second [or first] floor of the mall" if the Google Maps directory has launched to help a user navigate indoors. (ECF No. 202, at 95–96.)

Google stores this data in a repository known as the "Sensorvault" and associates each data point with a unique user account. (ECF No. 201, at 130.) The Sensorvault contains a substantial amount of information. McGriff testified that the Sensorvault assigns each device a unique device ID—as opposed to a personally identifiable Google ID—and receives and stores *all* location history data in the Sensorvault to be used in ads marketing. Google then builds aggregate models within the Sensorvault with data that is transformed so that it no longer looks like user data, and then uses the data to, for instance, assist decision-making in Google Maps. As another example, Google uses this data to depict whether certain locations are busy during particular hours. Both McGriff and Rodriguez declared that, to identify users within the relevant timeframe of a geofence, Google has to compare *all* the data in the Sensorvault in order to identify users within the relevant timeframe of a geofence. (ECF No. 96-1, at ¶ 23 ("Google must search across *all* [Location History] data," and "run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant."); ECF No. 96-2, at ¶ 7 ("Google must conduct the search across *all* [Location History] data.").) Clearly, however, Google can alter the data back to identify users in response to a geofence warrant.

Still, Location history is off by default. A user can initiate, or opt into, Location History either at the "Settings" Level, or when installing applications such as Google Assistant, Google Maps, or Google Photos. Although the specific software pathway each user sees at any given moment can differ based on numerous factors, McGriff acknowledged that it was "possible that a user would have seen the option" to opt into Location History multiple times across multiple apps. (ECF No. 202, at 77–78.) For instance, Google may prompt the user to enable Location History first in Google Maps, then again when he or she opens Google Photos and Google Assistant for the first time.[11]

Once a user opts into Location History, Google is "always collecting" data and storing *all* of that data in its vast Sensorvault, even "if the person is not doing anything at all with [his or her] phone." (ECF No. 201, at 114–15; *see* ECF No. 201, at 115 ("Once enabled, [Google is] now collecting [the user's] location history all the time.").) Even if a user enables Location History through an application and later deletes that app, Location History will "still collect[ ]" data on the user because Location History is tied to an individual's Google *account*, not to a *specific app*. (ECF No. 201, at 123–24.) Thus, after a user opts into the service, Location History tracks a user's location across every *app* and

---

[11] In a highly critical 2018 evaluation of tracking through Location History and Web & App Activity, the Norwegian Consumer Council (funded by the Norwegian government) characterized this as one of an identifiable set of problematic practices, dubbing it "repeated nudging" to encourage a user to enable the app. (Mar. 4–5 Hr'g Def. Ex. 27, at 28.)

every *device* associated with the user's account. Approximately one-third of all active Google users have Location History enabled on their accounts.

In certain circumstances, Google can estimate a device's location down to three meters. Location History cannot, however, pinpoint an individual's location with absolute precision. Instead, Google *estimates* a phone's coordinates. When Google, through Location History, reports a device's estimated location by placing a point on a map, it also depicts around that point a "confidence interval"—a circle of varying sizes—which indicates Google's confidence in its estimation. (ECF No. 201, at 38, 212; ECF No. 202, at 253–54.) The smaller the circle around a phone's estimated location, the more confident Google is in that phone's exact location, and *vice versa*. In general, "Google aims to accurately capture roughly 68 percent of users" within its confidence intervals. (ECF No. 201, at 213.) "[I]n other words, there[is] a 68 percent likelihood that a user is somewhere inside" the confidence interval. (ECF No. 201, at 213.)

ii. Web and App Activity

Web and App Activity collects a wider variety of information than Location History. If a user opts into WAA and has authorized all other requisite device permissions, WAA collects certain data points when a user *affirmatively engages* in certain activities.[12] For example, when a user performs a Google search, Google may, through WAA, keep a record of that search so that

[12] This stands in contrast to Location History, which constantly and *passively* logs a user's location.

it can "automatically suggest[ ]" that search to the user at a later time. (ECF No. 96-1, at ¶ 16.) Google maintains that WAA allows a user to "experience faster searches and more helpful app and content recommendations." (ECF No. 96-1, at ¶ 16.) "Some of [the data obtained through WAA] can include location information, although the source of the location information will vary depending on the activity, the device, and the user's other settings." (ECF No. 96-1, at ¶ 16.) Location History "and WAA are separate services that store data in separate databases." (ECF No. 96-1, at ¶ 16.) That is, "WAA data is not used to calculate the locations that are stored in [Location History], and completing a search across [Location History] data does not search or draw on WAA data in any way." (ECF No. 96-1, at ¶ 16.)

iii. Google Location Accuracy

Lastly, Google Location Accuracy—only available on Android devices[13]—allows a user's phone to draw in location data from sources other than GPS information. "If a user has the GLA setting on, the Android[device's] location services will use additional inputs, including Wi-Fi access points, mobile networks, and sensors[ ] to estimate the device's location." (ECF No. 96-1, at ¶ 17.) Thus, "the device 's location information that is sent to and stored in [Location History] ... may be calculated using not only GPS-sourced data, but also [more detailed] WiFi-or cell-sourced data from the GLA database." (ECF No. 96-1, at ¶ 17.) "In other words, GLA data might be used by the device to calculate a [more precise] location data point that is then stored in

[13] At the time of the robbery, Chatrie used an Android device.

[Location History]." (ECF No. 96-1, at ¶ 17.) Like WAA, Google generally stores GLA data separate from Location History information.

Again, as a general matter, Google appears to draw only from Location History to produce records for geofence requests, as WAA and GLA do not collect enough data points to pinpoint "devices within a certain period of time within a certain radius." (ECF No. 202, at 138; *see* ECF No. 201, at 211; ECF No. 96-1, at ¶¶ 20–22.) In keeping with this principle, here, Google only produced to law enforcement information from its Location History database.

b. Enabling Location History

The Court reports its understanding of the software pathways necessary to enable Location History based on two sets of sources. All sources agree that Chatrie enabled his Location History on July 9, 2018. However, even with input from two knowledgeable witnesses, the record as to how users can and do—and how Chatrie in particular could and did—enable Location History is not definitive on this record.

First, Defense Expert Spencer McInvaille testified in Court using a video of a device employing what was likely the same software used by Chatrie's phone to demonstrate how one might activate Location History through the Google account setup or through an app such as Google Maps. (Jan. 21 Hr'g Def. Ex. 4 ("Opt-In Video").) McInvaille also offered a written report explaining how Chatrie may have enabled location history. In that report, McInvaille reported that Chatrie

most likely enabled LH using Google Assistant, and that it was enabled on July 9, 2018.

Second, Google Location History Product Manager Marlo McGriff filed three declarations that explain how Google collects, stores, and turns over Location History data. He also testified in person during the March 4–5 Suppression Hearing. In his second declaration, McGriff concedes that McInvaille's video exhibit depicts largely accurate pathways to enable Location History. But McGriff states that McInvaille's video is incomplete. McGriff notes that "[b]y 2017 at the latest, it was not possible for a user to unable [Location History] solely by tapping on 'YES, I'M IN' as depicted on the final screen in the McInvaille Video." (ECF No. 110-1, at ¶ 7.) Instead, "a user who tapped on 'YES, I'M IN' ... would be presented with a second opt-in screen" described above. (ECF No. 110-1, at ¶ 7.) McGriff presents the Court with the exact text of the second opt-in screen in his Third Declaration.[14] (ECF No. 147, at ¶¶ 7–8; *see* ECF No. 147, at ¶ 10 ("The text quoted in ¶¶ 7–8 is the same text that [Chatrie] would have seen on July 9, 2018.").

No expert could say *exactly* which software pathway Chatrie would have seen when he enabled Location History, nor could Google determine which app he used to turn the service on. Google does, however, accept that

---

[14] McGriff complicated this seemingly straightforward proposition by acknowledging that any "device that has been sitting on a shelf for three years [would use start up language] dated to when it was baked into the device." (ECF No. 202, at 18.)

Chatrie would have seen the informational text in Part II.A.3.b.ii ("Through an App") in *some* form.

i. Through Phone Setup

As mentioned, a user must affirmatively enable Location History before Google uses the service to log the user's whereabouts. Google first allows users to enable Location History during the initial Google account setup process. After a new user connects the phone to the internet, agrees to the phone manufacturer's terms and conditions, and inputs the necessary information to create a Google account, the interface displays Google's terms of service. (*See* ECF No. 110-1, at ¶ 5 (acknowledging that the Opt-In Video exhibit was accurate but incomplete).) To move past this screen, the user must scroll through a summary of Google's privacy terms until the user reaches the bottom of the page. This page "does [not] ... say anything about [L]ocation [H]istory." (ECF No. 81, at 51.) Near the bottom, the screen displays blue text that reads, "MORE OPTIONS," with a downward-facing arrow next to the text. (Opt-In Video 3:00.) If the user taps on "MORE OPTIONS," the interface displays additional information about Google's location services. (ECF No. 81, at 51.) This additional information informs the user that WAA and GLA are enabled by default. Although Location History is *not* enabled by default, the user can opt into it from this screen by checking a box.

ii. Through an App

If a user does not enable Location History while setting up his or her Google account, Google will also prompt the user to turn the service on as soon as he or she sets up

an app "that has [Location History]-powered features." (ECF No. 110-1, at ¶ 5; *accord* ECF No. 96-1, at ¶¶ 3–6; ECF No. 201, at 221; ECF No. 202, at 8–9.) Such apps include Google Maps, Google Photos, and Google Assistant. When a user opens one of these apps for the first time, the phone immediately directs the user to a bright blue screen that reads: "Get the most from Google Maps." (Opt-In Video 4:36.) This screen informs the user that "Google needs to periodically store [his or her] location to improve route recommendations, search suggestions, and more." (Opt-In Video 4:36.) Below that, the interface offers the user the option to "LEARN MORE." (Opt-In Video 4:36.) If the user taps "LEARN MORE," the page redirects to "[a]ll of [Google's] terms and conditions"—but these terms and conditions include no information specifically tailored to location information. (ECF No. 81, at 57.)

Back at the initial blue page, the user can either select "YES, I'M IN" or "SKIP." (Opt-In Video 4:36.) As of July 2018, once the user selects "YES, I'M IN," the interface redirects the user to another page that displays the following text:

> **Location History**
>
> Saves where you go with your devices v [15]
>
> This data may be saved and used in any Google service where you were signed in to give you

---

[15] Although the testimony is unclear on the matter, prior to 2018, this line appears to have read: "[C]reates a private map of where you go with your signed in devices." (ECF No. 201, at 266.) Google changed this language in response to European regulation.

> more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

(ECF No. 147, at ¶ 7 (bold in original).) Next to "Location History: Saves where you go with your devices," the interface includes an "expansion arrow," depicted in the above text with a downward-facing caret. (ECF No. 147, at ¶ 8.) If a user "tap[s] on [this] expansion arrow," the interface "present[s the user] with additional information about" Location History. (ECF No. 147, at ¶ 8.) The screen then reads:

> **Location History**
>
> Saves where you go with your devices
>
> Location History saves where you go with your devices. To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, like Google Maps or Search.
>
> If you use your device without an internet connection, your data may be saved to your account once you return online.
>
> Not all Google services save this data to your account.
>
> This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google.

> This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

(ECF No. 147, at ¶ 8 (bold in original).) If the user selects "TURN ON"—either in the original screen or this expanded version—Location History is enabled. (ECF No. 147, at ¶ 9.) Importantly, a user need not interface with or employ the expansion arrow to enable Location History. In other words, a user could activate the service without knowing any of the further details of the service as explained in the above expanded version.

As noted, Chatrie enabled Location History on his device on July 9, 2018 at 12:09 a.m. Eastern Standard Time, and he appears to have done so through Google Assistant.

c. "Pausing" and Trying to Delete Location History

After a user opts in, he or she has two mechanisms to manage Google's collection and retention of his or her Location History data: "pausing" the service, or deleting the information it collected.

i. Pausing

As Google Location History Product Manager Marlo McGriff explained, when a user "*pauses*" his or her Location History, it merely "halts the collection of future data;" *it does not delete* information Google has already

obtained. (ECF No. 202, at 84.) And deleting an app through which the user enabled Location History will not pause the service.

A user may pause Location History on an Android device in one of three locations. First, the user can pause it "through the settings on any particular app that uses Location History." (ECF No. 202, at 63.) Second, he or she can pause it by navigating "through the device level settings." (ECF No. 202, at 63.) Finally, the user can log into myactivity.google.com and change his or her location settings. For each of these options, "a user [must] actively, intentionally navigate" through each interface. (ECF No. 202, at 64.)

When a user attempts to pause Location History, the device will present a pop-up screen containing text called the "pause copy." (Mar. 4–5 Hr'g Def. Ex. 27, at 23.) The pause copy warns users that pausing Location History will "limit[ ] functionality of some Google products over time, such as Google Maps and Google Now." (Mar. 4–5 Hr'g Def. Ex. 27, at 23; *accord* ECF No. 202, at 66.) Yet the record suggests that apps such as Google Assistant *will* continue to function with Location History paused. For instance, McInvaille noted that, despite prompts from Google to initiate Location History because apps like Google Assistant "depen[d] on these settings in order to work correctly," the user does not "need Location History for [Google Assistant] to work." (ECF. No. 201, at 111, 113.)

The pause copy also does not specifically detail how app functionality might be limited. Nor does Google inform users of the fact that the app will, indeed, continue to

function without Location History enabled, either when setting up the application or when displaying the pause copy. McGriff confirmed that when a user "pauses" the service, it halts only the collection of future data, and it does not (if a user has opted in) pause other location services such as Web & App Activity. (ECF No. 202, at 84, 90.)

ii. Trying to Delete

In 2018, when Chatrie enabled his Location History, a user had only one option to *delete* his or her Location History: by visiting myactivity.google.com and viewing his or her Timeline. Through the Timeline, a user "can review, edit, or delete [his or] her [Location History data] at will." (ECF No. 96-1, at ¶ 15.) But in response to an article from the Associated Press criticizing Google's acquisition of location data, one Google employee apparently remarked through an email: "The current [User Interface as of August 13, 2018] *feels* like it is designed to make things *possible*, yet *difficult* enough that people won't figure ... out" how to turn Location History off.[16] (Mar. 4–5 Hr'g Def. Ex. 30, at 6 (emphasis added).) Whether the substance of this remark is true or

[16] On May 11, 2018, two Senators launched an investigation into Google's acquisition of location data. During the March 4–5 Suppression Hearing, Chatrie tried to suggest that this investigation—in conjunction with a critical article from news website Quartz—*caused* Google to issue an update to its privacy policy on May 25, 2018. Google's expert McGriff testified credibly, however, that the investigation and policy changes were unrelated, because "there[was] no way Google updated its privacy policy in two weeks." (ECF No. 201, at 259.)

not, the sentiment it expresses is certainly not inconsistent with the record before the Court.

The effort to clarify this interface obviously is ongoing at Google.[17] In May 2019, McGriff formally heralded the "autodelete" controls that made it easier for users to manage their data. (*See* Mar. 4–5 Hr'g Def. Ex. 46.) And in December of 2019, McGriff introduced, on behalf of Google, "Incognito mode" and "Bulk delete in Timeline." (*See* Mar. 4–5 Hr'g Def. Ex. 47.)

---

[17] Since 2018, Google has added another feature to increase user control over Location History data. It now allows a user to set an "auto delete function" that limits how long Location History information remains with Google. (Mar. 4–5 Hr'g Def. Ex. 46, at 2.) The auto delete function now enables a user to "[c]hoose a time limit" for how long he or she wants Google to save activity data and "any data older than that will be automatically deleted from [the] account on an ongoing basis." (Mar. 4–5 Hr'g Def. Ex. 46, at 2.) McGriff testified that Google has also now developed a practice whereby Google sends monthly or annual emails about how to change settings. Google has no record that these emails were ever sent to Chatrie.

Still, concern about the user interface seemed to persist over time. Chatrie presented what purported to be emails from Google employees (garnered for other litigation) noting the confusing nature of various location products. One, in April 2019, reads: "Speaking as a user, WTF? More specifically I **thought** I had location tracking turned off on my phone. However the location toggle in the quick settings was on. So our messaging around this is enough to confuse a privacy focused Google-[software engineer]. That's not good." (Mar. 4–5 Hr'g Def. Ex. 37, at 5). The Norwegian report called this phenomenon "[d]eceptive click-flow." (Mar. 4–5 Hr'g Def. Ex. 27, at 27).

d. Google's Process in Answering a Geofence Warrant

Geofence warrants represent "a novel but rapidly growing [investigatory] technique." (ECF No. 59-1, at 8.) When law enforcement seeks a geofence warrant from Google, it (1) identifies a geographic area (also known as the "geofence," often a circle with a specified radius), (2) identifies a certain span of time, and (3) requests Location History data for all users who were within that area during that time. (*See* ECF No. 96-2, at ¶ 4.) The requested time windows for these warrants "might span a few minutes or a few hours." (ECF No. 96-2, at ¶ 4.)

In recent years, the number of geofence warrants received by Google has increased exponentially. Google received its first in 2016. After that, Google "observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and the rate ... increased over 500% from 2018 to 2019." (ECF No. 59-1, at 8.) In 2019, Google received "around 9,000 total geofence requests."[18] And Google now reports that geofence warrants comprise more than twenty-five percent of *all* warrants it receives in the United States. Google, *Supplemental Information on Geofence*

[18] To clarify, a geofence *request* is not identical to a geofence *warrant*. "[I]n some cases, law enforcement is[not] aware that [it] need[s] to submit a warrant" to obtain Location History. (ECF No. 202, at 173.) Google still considers this communication from law enforcement a "geofence request," even when not accompanied by a warrant. (ECF No. 202, at 173.)

Warrants in the United States (last visited Mar. 1, 2022), https://bit.ly/3o7Znqc.

Google began to take issue with certain early geofence warrants because the requests were too broad. As related by Legal Investigations Specialist Rodriguez, the warrants "sought [Location History] data that would identify *all* Google users who were in a geographical area in a given time frame." (ECF No. 96-2, at ¶ 5 (emphasis added).) Thus, in 2018, Google held both internal discussions with its counsel and external discussions with law enforcement agencies, including the Computer Crime and Intellectual Property Section of the United States Department of Justice ("CCIPS"), to develop internal procedures on how to respond to geofence warrants. "To ensure privacy protections for Google users, ... Google instituted a policy of objecting to any warrant that failed to include de[-]identification and narrowing measures." (ECF No. 96-2, at ¶ 5.) Seemingly developed as a result of Google's collaboration with CCIPS, this de-identification and narrowing "protocol typically ... entails a three-step process." (ECF No. 96-2, at ¶ 5; *see* ECF No. 202, at 553.) As noted earlier, the Court draws its understanding of this process from an amalgam of in-person testimony and a declaration submitted by current Google Tooling and Programs Lead and former Legal Specialist Sarah Rodriguez.

i. Step 1

First, at Step 1, law enforcement receives a warrant "compelling Google to disclose a *de-identified* list of all Google user[s]" whose Location History data indicates were within the geofence during a specified timeframe.

(ECF No. 96-2, at ¶ 6 (emphasis added).) In response to the warrant, Google must "search ... *all* [Location History] data to identify users" whose devices were present within the geofence during the defined timeframe. (ECF No. 96-2, at ¶ 7; ECF No. 96-1, at ¶ 23.) "Google does not know which users may have ... saved [Location History] data before conducting th[is] search." (ECF No. 96-2, at ¶ 7.)

Rodriguez stated that, as part of this first step, Google provides the Government with responsive user records identified in the Sensorvault. Google deems a record "responsive" if a user's estimated location (*i.e.*, the stored coordinates of the phone in Location History) falls within the boundaries of the geofence. (ECF No. 96-1, at ¶ 25.) Rodriguez confirmed that, for every device whose "stored latitude/longitude coordinates fall within the radius described in the warrant," Google turns over a "'production version' of the [users'] data." (ECF No. 96-2, at ¶ 8.) This production version "includes a [de-identified] device number, [19] the latitude/longitude

---

[19] When responding to geofence warrants, Google:

> de[-]identifies the data produced to the [G]overnment at this [first] step by removing the [user's distinct] Google Account ID ..., leaving only a device number that is used only in the Location History database. This device number is only used for distinguishing devices reporting [Location History] to a user's account ...

(ECF No. 96-2, at ¶ 9.) Unlike a Google Account ID, a Location History device number does not by itself identify which account is associated with certain location points. However, as discussed in Part II.A.6.b ("The Three Paths Video"), *infra*, piecing together an "anonymous" user's location data could reveal that user's identity.

coordinates and timestamp of the stored [Location History] information, the map's [confidence interval], and the source of the stored [Location History]," (*i.e.*, "whether the location was generated via Wi-Fi, GPS, or a cell tower"). (ECF No. 96-2, at ¶ 8.)

According to Rodriguez, the sizes and timeframes of geofences "vary considerably from one request to another." (ECF No. 96-2, at ¶ 8.) Because Google produces *all* location points captured within the geofence over the timeframe, "[t]he volume of data produced at [Step 1] depends on the size and nature of the geographic area and length of time covered by the geofence request." (ECF No. 96-2, at ¶ 8.) Google does not impose specific, objective restraints on the size of the geofence, the length of the relevant timeframe, or the number of users for which it will produce data.

Indeed, Google places significant discretion on the LIS employee who initially reviews a particular geofence warrant. This "specialist" will first process and review the warrant. (ECF No. 202, at 178–79.) If the specialist believes the warrant "needs further review"—for example, if the geofence seems too large or the timeframe too long—he or she may first "engage with [the requesting] law enforcement officer to collect more information about the investigation." (ECF No. 202, at 179, 182.) From there, the specialist will "consult with [Google's] legal counsel." (ECF No. 202, at 179.) If Google's counsel objects to the warrant, Google may have a "conversation" with law enforcement to alleviate Google's concerns, or it may "require law enforcement to obtain an amended or a newly-issued warrant that addresses the issue." (ECF No. 202, at 187.) Assuming

law enforcement eventually assuages Google's concerns with the warrant, Google then provides the Government with the de-identified geofence data.

ii. Step 2

Second, according to Rodriguez, at Step 2, the Government "reviews the de[-]identified [data] to determine the [Sensorvault] device numbers of interest." (ECF No. 96-1, at ¶ 10.) If law enforcement needs "additional de[-]identified location information for a [certain] device" to "determine whether that device is actually relevant to the investigation," law enforcement, at this step, "can compel Google to provide additional ... location coordinates *beyond* the time and geographic scope of the original request."[20] (ECF No. 96-2, at ¶ 10 (emphasis added).) These additional location points "can assist law enforcement in eliminating devices" from the investigation that were, for example, "not in the target location for enough time to be of interest, [or] were moving through the target location in a manner inconsistent with other evidence."[21] (ECF No. 96-2, at ¶ 11.) Notably, Google imposes "no geographical limits" on this Step 2 data. (ECF No. 202, at 184.) Thus, if a user's location fell within the geofence at Step 1, law enforcement can obtain *all* location points for identified users over an expanded timeframe at Step 2. This means

---

[20] At Step 2, for law enforcement to expand the timeframe from which to obtain Location History data, Google generally requires that the warrant explicitly expand that timeframe *in the warrant's text*. Otherwise, Google will object to that request.

[21] If law enforcement requests this additional data, it must typically do so within sixty days.

that, at Step 2, no geographic barrier confines the information searched.

Google does, however, typically require law enforcement to narrow the number of users for which it requests Step 2 data so that the Government cannot not simply seek geographically unrestricted data for *all* users within the geofence. Google has no firm policy as to precisely *when* a Step 2 request is sufficiently narrow. But if law enforcement requests "a lower number of devices from St[ep] 1 to St[ep] 2," this, to some extent, demonstrates to Google that law enforcement has tailored the data it seeks. (ECF No. 202, at 190.) Again, assuming Google has no further objections to law enforcement's Step 2 request, Google provides law enforcement with de-identified but geographically unrestricted data.

iii. Step 3

Finally, at Step 3, drawing from the de-identified data Google has produced so far, "the [G]overnment can compel Google ... to provide *account-identifying information*" for the users "the [G]overnment determines are relevant to the investigation." (ECF No. 96-2, at ¶ 12 (emphasis added).) [22] This "account-identifying information" includes the name and email address associated with the account. (ECF No. 96-2, at ¶ 12; ECF No. 202, at 192.) Google seems to prefer that law enforcement request Step 3 data on fewer users than requested in Step 2, although it is "[p]ossibl[e]" that

[22] Law enforcement has sixty days from the time Google turns over Step 2 data to request Step 3 information.

Google would approve a Step 3 request that is not narrowed after Step 2 at all. (ECF No. 202, at 194.)

4. The Instant Geofence Warrant and Its Justifications

a. Det. Hylton's Investigation[23]

When Det. Hylton responded to the scene of the bank robbery on May 20, 2019, he "interviewed witnesses" and "reviewed surveillance camera video from ... the Call Federal Credit Union Bank." (ECF No. 202, at 330.) Through this initial investigation, he "learned that [the] suspect had come from the southwestern corner of the Journey Christian Church [the 'Church'], ... a building adjacent and to the east of the Call Federal Credit Union, at approximately 4:50 in the afternoon." (ECF No. 202, at 330–31.) He also learned of the core facts that underlie this case—that the suspect walked into the Bank wearing a fisherman's hat and traffic vest, presented the teller with a note demanding $100,000, forced the manager at gunpoint to open the Bank's vault, took $195,000, and may have left in a blue Buick

[23] Although the subsequent warrants evaluated in a separate Opinion, explain officers' investigatory efforts to identify a suspect beyond reviewing security camera footage, the Geofence Warrant contains no information about those efforts. Because the Geofence Warrant does not expressly incorporate these subsequent warrants—and indeed, it could not have because officers obtained them after drafting the Geofence Warrant—the Court will consider only the following facts in its analysis. *SeeUnited States v. Hurwitz*, 459 F.3d 463, 470 (4th Cir. 2006) (requiring that a warrant either incorporate a supporting document by reference or attach the document to warrant itself in order for a court to read the document alongside the warrant).

Lacrosse. Critically, through security footage, Det. Hylton observed that when the suspect first walked into Bank, he was "holding what appeared to be ... a cell phone to the side of his face." (ECF No. 202, at 331.) To Det. Hylton, this use of a phone suggested "that [the suspect] could have possibly been speaking with a coconspirator." (ECF No. 202, at 333.)

After Det. Hylton completed his on-site investigation, he pursued at least two other leads. First, a purportedly estranged romantic partner called the police and told them that she "kn[e]w who did th[e] robbery," and that the suspect was her "ex-boyfriend." (ECF No. 202, at 334.) Law enforcement found this ex-boyfriend, interviewed him, examined his cell phone, and ultimately determined that he was not the suspect. Next, an employee at another branch of the Bank alerted the police about an individual who drove a blue Buick Lacrosse and wore a traffic vest. Det. Hylton ultimately determined that this individual was likewise not the suspect.

Having unearthed no further leads from his investigation, Det. Hylton then turned to geofence technology. He had sought three other geofence warrants in the past. Before seeking those warrants, he had consulted with prosecutors, who approved them. Magistrates—including one federal magistrate judge—approved all three as well. Those warrants were, according to Det. Hylton, "mostly similar" to the one at bar. (ECF No. 202, at 328; *compare* Mar. 4–5 Hr'g Def. Ex. 18 ("Prior Federal Geofence Warrant") and Mar. 4–5 Hr'g Def. Ex. 19 ("Prior State Geofence Warrant") *with* ECF No. 54-1.) Indeed, all but one adopted a

roughly 150-meter radius, although a "few of them had more locations because [there were] more robberies to investigate." (ECF No. 202, at 328; *see* Prior Federal Geofence Warrant; Prior State Geofence Warrant.)

On June 14, 2019, roughly three weeks after the robbery, Det. Hylton applied for and obtained the instant Geofence Warrant from Chesterfield County Magistrate David Bishop.

b. Magistrate Bishop

Chatrie contests the sufficiency of Magistrate Bishop's qualifications. Although the Court will address that issue more fully later in this Opinion, the Court briefly notes that Chesterfield County Magistrate "David Bishop graduated from Pensacola Christian College with a Bachelor's of Science in Criminal Justice in May 2016."[24] (ECF No. 156, at 1.) Around two years later, on June 12, 2018, the Executive Secretary of the Supreme Court of Virginia appointed Bishop as a magistrate. Magistrate Bishop completed his statutorily required probationary period on March 12, 2019. He was released for service on October 24, 2018.

---

[24] The Virginia Code imposes one educational requirement on the Commonwealth's magistrates: they must possess a bachelor's degree "from an accredited institution of higher education." Va. Code § 19.2-37. The Code does not further define what qualifies as an "accredited institution" for the purpose of magistrates. Chatrie disputes whether Magistrate Bishop's alma mater, Pensacola Christian College, is sufficiently "accredited" under the Virginia Code. (ECF No. 135, at 6–9.) The Court will speak to this later in the Opinion.

Three months after Magistrate Bishop finished his probationary period, Det. Hylton presented Magistrate Bishop with the instant Geofence Warrant. When Magistrate Bishop reviewed the Warrant, he asked no questions of Det. Hylton, nor did he "seek to modify anything in the affidavit." (ECF No. 202, at 362.) Based on Det. Hylton's understanding, Magistrate Bishop simply "read [the Warrant] and signed it."[25] (ECF No. 202, at 362.) The record suggests that this was the first geofence warrant Magistrate Bishop had signed.

c. The Instant Geofence Warrant

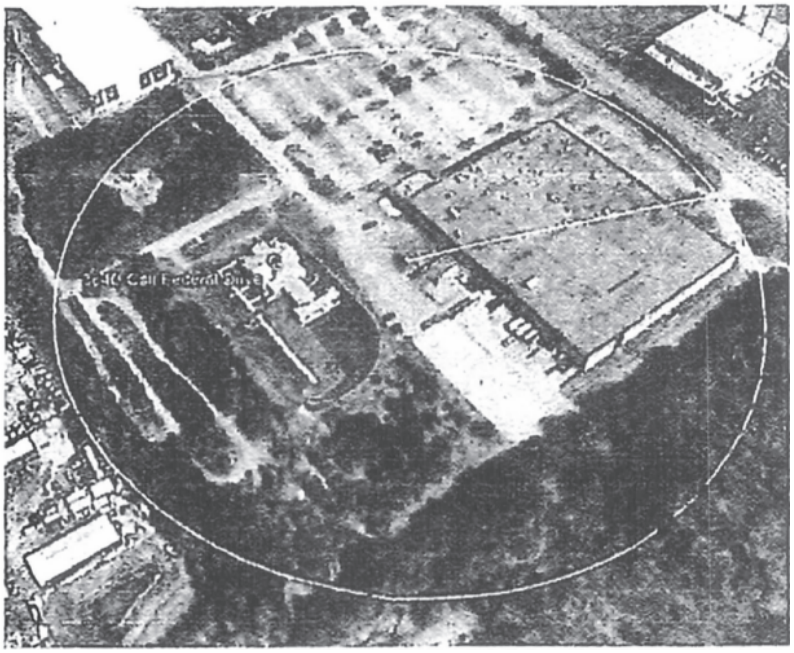
The Warrant drew a geofence with a 150-meter radius—with a *diameter* of 300 meters, longer than three football fields—in an urban environment which included the Bank and the nearby Journey Christian Church.[26] All told, the geofence encompassed 17.5 acres. The eastern side of the geofence abutted but did not include Price Club Boulevard. The southern side encompassed a wooded area behind the Bank. The northern side encircled the Church's parking lot, and the western side captured a wooded area to the west of the Bank. The

---

[25] Det. Hylton did note, however, that because Magistrate Bishop did not read the Warrant in front of him, Magistrate Bishop "*could* have consulted with someone" about it. (ECF No. 202, at 362 (emphasis added).)

[26] Thus, the total area of the geofence is 70,686 square meters—about three and a half times the *footprint* of a New York city block. Michael Kolomatsky, *How Big Is an Acre, Anyway?* N.Y. Times (July 26, 2018), https://nyti.ms/345CjS7. Of course, this portion of suburban Richmond, Virginia does not have the density (or height) comparable to that of seven New York City blocks.

Warrant included the following photograph of the area with the geofence superimposed over it:



The Warrant sought location data for every device present within the geofence from 4:20 p.m. to 5:20 p.m. on the day of the robbery. In keeping with Google's established approach, the Geofence Warrant described a three-step process by which law enforcement would "attempt to narrow down" the list of users for which the Government would obtain the most invasive information. (ECF No. 54-1, at 4.)

At Step 1, "Google w[ould] provide 'anonymized information' regarding the Accounts that are associated with a device that was inside the described geographical area" from 4:20 p.m. to 5:20 p.m. (ECF No. 54-1, at 4.) At

Step 2, "Law enforcement w[ould] return a list [of accounts] that they ha[d] attempted to narrow down." (ECF No. 54-1, at 4.) Google would then "produce contextual data points with points of travel outside of the geographical area." (ECF No. 54-1, at 4.) During Step 2, the warrant expanded the timeframe to include thirty minutes before and thirty minutes after the initial hour-long window, so that the Step 2 window was two hours long in total. (ECF No. 54-1, at 4.) Finally, at Step 3, after Government review, Google would "provide identifying account information/CSI[27] for the accounts requested" by law enforcement. (ECF No. 54-1, at 4–5.)

In explaining why "Google [should] provide Geo[f]encing data," Det. Hylton noted in the warrant's accompanying affidavit that:

> when people act in concert with one another to commit a crime, they frequently utilize cellular telephones and other such electronic devices, to

---

[27] The warrant included in the definition of "identifying account information/CSI" the following:

> user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used to set up the account, verify the account or to receive assistance with the account, and Google Voice phones numbers associated with the account.

(ECF No. 54-1, at 4.)

> communicate with each other through WiFi, Bluetooth, GPS, voice calls, text messages, social media accounts, applications, emails, and/or cell towers in the area of the [crime].

(ECF No. 54-1, at 6.) Specifically, he noted that when reviewing the Bank's surveillance footage, he observed that the perpetrator "had a cell phone in his right hand and appeared to be speaking with someone on the device." (ECF No. 54-1, at 6.) He further explained that:

> Google has ... developed a proprietary operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.
>
> Based on [his] training and experience, [he has learned] that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled.

ECF No. 54-1, at 7.) Therefore, he explained, "the requested data/information would have been captured by Google during the requested time." (ECF No. 54-1, at 6.) Det. Hylton noted several ways law enforcement could use this information. For example, "location data ... may tend to identify potential witnesses and/or suspects." (ECF No. 54-1, at 7.) In turn, this geographic

and timeline information may tend to "inculpat[e] or exculpate[e] persons of interest." (ECF No. 54-1, at 7.)

Inexplicably, on June 19, 2019—*the day before he sent the Warrant to Google*—Det. Hylton submitted his return for the Warrant to the Chesterfield County Circuit Court. A search warrant return "notifies the Court when [an officer] *execute*[*s*] a search warrant," and the officer "report[s] back to the Court what items [he or she] gathered during the search." (ECF No. 202, at 366-68 (emphasis added).) In the return, he stated that he had executed the warrant on June 14, 2019. Yet he had not yet sent the Warrant to Google. Moreover, in describing the items *already seized* under the Warrant—again, he had not yet executed it—Det. Hylton wrote for what would be a sizable amount of precise location information on at least nineteen device users: "Data." (Mar. 4–5 Hr'g Gov't Ex. 2, at 9; *see* ECF No. 202, at 367, 369); *see also United States v. Williams*, 592 F.3d 511, 520 (4th Cir. 2010) ("While the [Fourth Amendment's] protection cannot demand perfection, any tolerance of imperfection does not give officers free reign to ransack and take what they like." (citation and quotation marks omitted)).

5. Google Receives the Geofence Warrant

The next day, on June 20, 2019, Det. Hylton sent Google the Warrant that Magistrate Bishop had approved. Pursuant to Step 1, Google produced anonymized Location History data for all accounts associated with phones present within the geofence from 4:20 p.m. to

5:20 p.m.—nineteen users in total.[28] Associated with these nineteen users were 210 individual location points, along with the confidence interval for each point. In this case, law enforcement ran this information through a program to produce a visual representation of the data. *See* Part II.A.6.a, *infra.*

A few days after Google provided him the Step 1 information, Det. Hylton emailed Google. The record then strongly suggests that he did not "attempt to narrow down" the list of devices for which he requested further data. In contravention to Google's policy, and without consulting Magistrate Bishop, Det. Hylton requested "additional location data" (Step 2 data) *and* "subscriber information" (Step 3 data) "for *all* 19 device numbers produced in [S]tep 1." (ECF No. 48-1, at 1; *accord* ECF No. 96-2, at ¶ 15; ECF No. 202, at 195, 345.) He noted that, because "the sought Google devices [were] fairly low in number," he requested Step 2 and 3 data for *all* nineteen users "in an effort to rule out possible co-conspirators." (ECF No. 48-1, at 1; *see* ECF No. 202, at 195.) He admitted, however, that "device numbers 1–9 may fit the more likely profile of [the]

---

[28] Google provides this information in a table, sorted into seven columns: "Device ID," "Date," "Time," "Latitude," "Longitude," "Source," and "Maps [Confidence Interval]." (*See*, *e.g.*, Mar. 4–5 Hr'g Def. Ex. 3, at 7.) Google LIS Rodriguez testified that the Device ID is not an identifier for "any other specific Google account." (ECF No. 202, at 176.) It is not cross-referenced by Google outside of Location History, but if an individual device were responsive to two different geofence warrants, the ID would be the same in both. Law enforcement does not return this information to Google nor, in this case, did it return the data to the Chesterfield County Court.

parties involved." (ECF No. 48-1.) Six days after sending the email, Det. Hylton called Google and left two voicemails seeking a response.

A Google specialist then called Det. Hylton. As described by Rodriguez, the LIS "explained the issues" with Det. Hylton's request—namely, that the request "did not appear to follow the three sequential steps or the narrowing required by the search warrant." (ECF No. 96-2, at ¶ 16; *see* Mar. 4–5 Hr'g Tr. 189, 197.) "Det. Hylton asked ... what information would be produced in [S]tep 2 and ... [S]tep 3." (ECF No. 96-2, at ¶ 16.) The Google specialist explained the nature of the data to be turned over during these steps and emphasized to Det. Hylton "the importance of [S]tep 2 in narrowing." (ECF No. 96-2, at ¶ 16; *see* ECF No. 202, at 197.) The specialist, however, does not appear to have provided Det. Hylton with any "specific directive[s] ... about how much [Det. Hylton] had to narrow" his request. (ECF No. 202, at 197.) On July 9, 2019, Det. Hylton emailed Google, requesting Step 2 data on the *nine* users identified in his prior email. Google then provided him that information in the same format as Step 1 data had been returned. It does not appear that Det. Hylton explained to Google precisely why he requested Step 2 data for these nine particular accounts. Neither Det. Hylton nor Google consulted with a magistrate or judge before Google disclosed this data.

"On or about July 10, 2019, and July 11, 2019, Google received emails from [Det.] Hylton requesting [Step 3] information ... on [three] device numbers." (ECF No. 96-2, at ¶ 19.) Google provided him with this information—"the account subscriber information associated with the

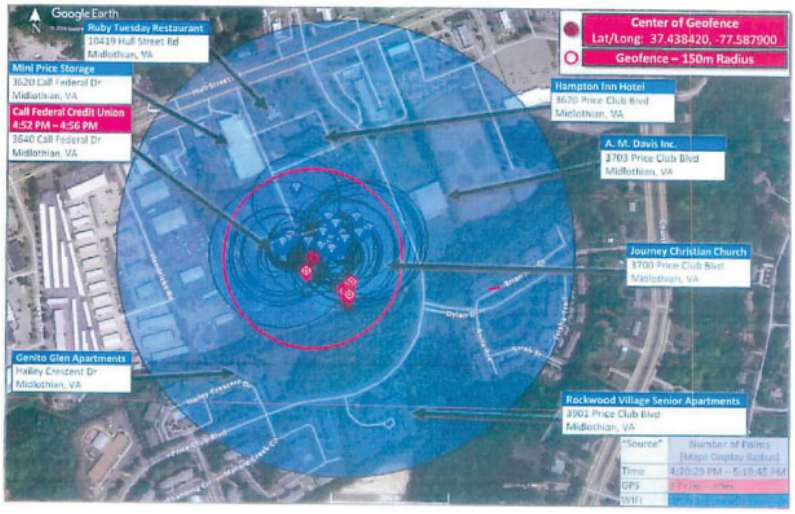
3 device numbers"—on July 11. (ECF No. 96-2, at ¶ 20.) Again, it is not apparent from the record whether Det. Hylton demonstrated to Google why he requested Step 3 data for these three accounts, nor did he seek the magistrate's approval before obtaining the data.

Finally, "[o]n or about July 12, 2019," Det. Hylton emailed Google "requesting *additional* device or phone number information that could be associated with one of the accounts" for which Google had produced Step 3 data. (ECF No. 96-2, at ¶ 21 (emphasis added).) This would have been an unauthorized Step 4. A Legal Investigations Specialist called Det. Hylton, that day and told him that "no further information was produced under" the Geofence Warrant. (ECF No. 96-2, at ¶ 21.)

6. Data Derived from the Warrant

a. Law Enforcement's Demonstrative

Upon receipt of the geofence data, law enforcement "imported [the Step 1 information] into mapping software" so that law enforcement could visualize the data points. (Mar. 4–5 Hr'g Gov. Ex. 1, at 15.) That program rendered the following depiction:



The visualization, created by Agent D'Errico, plots each point's confidence interval—the area in which Google is 68 percent confident a given individual is located—with a blue shaded circle.

Here, the largest confidence interval for a user located within the geofence had a radius of roughly 387 meters (longer than four football fields)—more than twice as large as the original geofence.[29] Thus, the Geofence

[29] The Court acknowledges that as a matter of fact, it is unlikely that this user would have been located far outside the geofence. As FBI Agent D'Errico testified during the March 4-5 Suppression Hearing, this user first reported a location point within the geofence with a confidence interval of around 84 meters. The next location point, reported only thirty seconds later, was the point with the 387-meter confidence interval—but the user's reported location was in exactly the same spot as the prior point. It is thus unlikely that the user would have traveled from an area in or near the geofence to a location significantly outside of it within thirty seconds. FBI Agent D'Errico did note, however, that these location points were "indicative ... that the device [was] moving," and that "for some

Warrant *could* have captured the location of someone who was hundreds of feet outside the geofence. Within this confidence interval—in addition to the Bank and the Church—are several buildings (with an unknown number of floors), including a Ruby Tuesday restaurant, a Hampton Inn Hotel, several units of the Genito Glen apartment complex, a self-storage business, a senior living facility, two busy streets (Hull Street and Price Club Boulevard), and what appear to be several residences near the southeast edge of the confidence interval. Near the time of the robbery, the individual whose account produced this large confidence interval could have been present at any of these locations instead of within the geofence.

Indeed, given that Google returns locations via these estimated location points, both McInvaille and D'Errico confirmed geofences can return both false positives (someone who is not in the geofence reported as being there) and false negatives (someone in the geofence not reported). Chatrie created a video based on the returns of this geofence warrant suggesting that a false positive was returned here.

b. The Three Paths Video

Chatrie's video depicting the movement of three phones was based on the data obtained through the Warrant at Step 2. At the March 4–5 Suppression Hearing, Chatrie

---

reason, ... a new center coordinate was not obtained by that phone." (ECF No. 202, at 255.) Nevertheless, the notion that geofences *can* capture information from users who are not even in the vicinity of the relevant area troubles the Court and evinces how broad a sweep these warrants may have.

introduced a video that plotted the locations of three anonymous individuals whose location data Google turned over at Step 2—"Mr. Blue," "Mr. Green," and "Ms. Yellow." (ECF No. 201, at 63, 67; *see* Mar. 4–5 Hr'g Def. Ex. 5 ("Three Paths Video").)

At the beginning of the two-hour, geographically unlimited, window for which the Government requested Step 2 location data, a cluster of location points for Mr. Blue appeared at a nearby apartment complex. At 4:34 p.m., Mr. Blue seemed to leave the apartment complex, and at 4:35 p.m., Mr. Blue's location estimate appeared inside the geofence, roughly seventeen minutes before the robbery occurred. However, at 4:36 p.m.—twenty-seven seconds later—Mr. Blue appeared outside the geofence on Price Club Boulevard, and by 4:37 p.m., Mr. Blue appeared to be driving down Hull Street. Mr. Blue then drove south and stopped at another residence—clustering location data for five minutes—and eventually drove back toward the original apartment complex, where he remained for the rest of the two-hour window. Because Mr. Blue appeared within the geofence for such a brief period of time—and because he appeared within the fence just as he appeared to drive on a nearby street—Defense Expert Mclnvaille testified that Mr. Blue may have been a "false positive"—he may not have actually stepped foot within the geofence. (ECF No. 201, at 43–44, 65.)

Mr. Green's location points initially clustered at a hospital for a period of about thirty-five minutes. Eventually, Mr. Green drove south along Old Courthouse Road, ultimately appearing inside the geofence at 4:41 p.m. Around two minutes later—and

nine minutes before the robbery—Mr. Green's estimated location appeared in a residential neighborhood, clustering around one home for the remainder of the two-hour window.

Finally, Ms. Yellow clustered location points at a house from 3:51 p.m. to 4:11 p.m. At 4:18 p.m., she clustered several points near a school, and by 4:26 p.m., she appeared to drive toward the Bank. At 4:31 p.m., she first appeared in the geofence, her location estimate surfacing inside the Bank. She reported two more location points inside the Bank, and by 4:36—eighteen minutes before the robbery—appeared to be driving away from the Bank. She drove south, arrived at the house from which she started, and remained there for the rest of the two-hour window.

Defense Expert McInvaille testified that he was able to access publicly available information such as tax records related to the homes in which Mr. Blue, Mr. Green, and Ms. Yellow appeared to spend significant time. He explained that these records, in conjunction with other publicly available information such as social media accounts, would have allowed him to determine these individuals' likely identities with only a few data points. Law enforcement would, of course, have similar or enhanced research capabilities to identify users based on these "de-identified" location points.

* * *

Ultimately, the Step 3 information law enforcement obtained led the authorities to Chatrie.

B. Procedural History

On September 17, 2019, a grand jury indicted Chatrie on two counts: (1) Forced Accompaniment During Armed Credit Union Robbery, in violation of 18 U.S.C. §§ 2113(a), (d), and (e); and, (2) Using, Carrying, or Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A). The police issued a warrant, and a magistrate judge signed a Petition and Order for Writ of Habeas Corpus ad Prosequendum ordering that Chatrie, then an inmate at Riverside Regional Jail, appear in the United States District Court for the Eastern District of Virginia to answer for the charges.

On October 1, 2019, Chatrie appeared before the magistrate judge and waived his right to a detention hearing. The magistrate judge ordered Chatrie detained pending trial. On that same day, Chatrie appeared for an arraignment and pleaded not guilty to the charged offenses.

On October 29, 2019, Chatrie filed the instant Geofence Motion to Suppress. (ECF No. 29.) The United States responded, (ECF No. 41), and Chatrie replied, (ECF No. 48). On December 23, 2019, the Court granted Google leave to file an amicus brief. (ECF No. 73.) In response to Chatrie's Federal Rule of Civil Procedure 17(c) subpoenas, Google also filed a total of four declarations by two Google employees: three by Marlo McGriff, and

(2) one by Sarah Rodriguez. (ECF Nos. 96-1, 96-2, 110-1,[30] 147.)

On November 9, 2020, around one week before the scheduled Suppression Hearing, Google filed a Motion for Leave to Present Remote Testimony. On November 11, 2020, Chatrie responded in opposition. In this response, Chatrie argued that "[i]n person testimony from the Google employees [was] critical to the Court's resolution of Mr. Chatrie's geofence warrant," and that "Google's continued intrusion into this case warrants a finding from this Court that the Google witnesses are hostile/adverse witnesses." (ECF No. 166, at 1, 6.) After the Court held a status conference on the Motion for Leave to Present Remote Testimony, Chatrie filed a Motion to Continue the November 17, 2020 hearing, seeking to continue the hearing to a time when Google would be able to attend in person. On December 18, 2020, the Court granted Chatrie's Motion to Continue and scheduled the Suppression Hearing for March 4, 2021.

Considering the novel and complex questions of law at issue, the Court allowed the parties to provide supplemental briefing on discovery provided by Google

---

[30] On June 17, 2020, Google sought leave to file a Supplemental Declaration of Marlo McGriff (the "Motion for Leave"). The Court granted the Motion for Leave over Chatrie's objection. Given the close proximity in time, the Court continued the then-scheduled July 2, 2020 geofence hearing. The Court found that "the ends of justice [were] best served by granting a short continuance" because "the Geofence Motion to Suppress presents substantial issues of first impression that require the Court to consider a full and accurate record concerning the technology at issue." (ECF No. 115, at 4.) The Court continued the hearing to November 17, 2020.

and the March 4-5, 2021 Suppression Hearing. Among others, witnesses from Google—McGriff and Rodriguez—provided the Court with a relatively exhaustive picture of Google's typical response to geofence warrants. Now, after careful consideration of the issues and with the aid of the parties' thorough briefing, the Court concludes that, although this warrant is invalid for lack of particularized probable cause, the Court cannot suppress the resulting evidence because the *Leon* good faith exception applies.

III. Analysis

Chatrie seeks to suppress evidence obtained from the June 14, 2019 Geofence Warrant that covered 70,686 square meters of land around the Bank, located in a busy part of the Richmond metro area. Despite the Court's concerns about the validity of this warrant and the adoption of unsupervised geofence warrants more broadly, the Court will deny Chatrie's Motion to Suppress because the officers sought the warrant in good faith.

A. The Court Will Briefly Address Fourth Amendment Standing

Because the Court will independently deny Chatrie's motion to suppress by considering the validity of the Geofence Warrant, the Court "need not wade into the murky waters of standing," *i.e.*, whether Chatrie has a reasonable expectation of privacy in the data sought by the warrant. *United States v. James*, No. 18cr216, 2018 WL 6566000, at *4 (D. Minn. Nov. 26, 2018); *see Byrd v. United States*, —— U.S. ——, 138 S. Ct. 1518, 1530, 200

L.Ed.2d 805 (2018) (Fourth Amendment standing "is not a jurisdictional question and hence need not be addressed before addressing other aspects of the merits of a Fourth Amendment claim.").

Nonetheless, the Court notes its deep concern (underlying both Fourth Amendment standing, and the third-party doctrine discussed below) that current Fourth Amendment doctrine may be materially lagging behind technological innovations. As Fourth Amendment law develops in a slow drip, "technology [continues to] enhance[ ] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes." *Carpenter v. United States*, —— U.S. ——, 138 S. Ct. 2206, 2214, 201 L.Ed.2d 507 (2018). Relevant here, although *law enforcement* limited the warrant's window to two hours, Google—despite efforts to constrain law enforcement access to its data—retains constant, near-exact location information for each user who opts in. *See* Part II.A.3.a, *supra.* The Government thus has an almost unlimited pool from which to seek location data, and "'[w]hoever the suspect turns out to be,' they have 'effectively been tailed'" since they enabled Location History. *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (en banc) (quoting *Carpenter*, 138 S. Ct. at 2218).

Indeed, the "'retrospective quality of [geofence] data' enables police to 'retrace a person's whereabouts,'" and "[p]olice need not even know in advance whether they want to follow a particular individual, or when." *Id.* at 342 (quoting *Carpenter*, 138 S. Ct. at 2218). Until recently, the ease with which law enforcement might access such precise and essentially real-time location

data was unimaginable. And it is this expansive, detailed, and retrospective nature of Google location data that is unlike, for example, surveillance footage, and that perhaps causes such data to "cross[ ] the line from merely augmenting [law enforcement's investigative capabilities] to impermissibly enhancing" them. *Id.* at 341.

What is more, the Court is disturbed that individuals other than criminal defendants caught within expansive geofences may have no functional way to assert their own privacy rights. Consider, for example, a geofence encompassing a bank, a church, a nearby residence, and a hotel. Ordinarily, a criminal perpetrator would not have a reasonable expectation of privacy in his or her activities within or outside the publicly accessible bank. *See United States v. Knotts*, 460 U.S. 276, 281, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). He or she thus may not be able to establish Fourth Amendment standing to challenge a time-limited acquisition of his location data at the bank.

But the individual in his or her residence likely *would* have a heightened expectation of privacy. *Silverman v. United States*, 365 U.S. 505, 511, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961) ("At the very core [of the Fourth Amendment] stands the right of a [person] to retreat into his [or her] own home and there be free form unreasonable government intrusion."). Yet because that individual would not have been alerted that law enforcement obtained his or her private location information, and because the criminal defendant could

not assert that individual's privacy rights in his or her criminal case, *United States v. Rumley*, 588 F.3d 202, 206 n.2 (4th Cir. 2009), that innocent individual would seemingly have no realistic method to assert his or her own privacy rights tangled within the warrant. Geofence warrants thus present the marked potential to implicate a "right without a remedy." *Hawkins v. Barney's Lessee*, 30 U.S. 457, 463, 5 Pet. 457, 8 L.Ed. 190 (1831) ("There can be no right without a remedy to secure it.").

As this Court sees it, analysis of geofences does not fit neatly within the Supreme Court's existing "reasonable expectation of privacy" doctrine as it relates to technology. That run of cases primarily deals with *deep*, but perhaps not *wide*, intrusions into privacy. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (considering the validity of using thermal imaging on one's home); *United States v. Jones*, 565 U.S. 400, 402-03, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (construing "the attachment of a [GPS] tracking device to an individual's vehicle" for twenty-eight days); *Carpenter*, 138 S. Ct. at 2217 n.3 (considering whether "accessing seven days of [an individual's cell site location information] constitutes a Fourth Amendment search").

At base, these matters are best left to legislatures. *See* Zach Whittaker, *A Bill to Ban Geofence and Keyword Search Warrants in New York Gains Traction*, TechCrunch (Jan. 13, 2022), https://tcm.ch/35mLHkP (discussing a recently introduced New York bill that would ban the use of geofence warrants statewide). This case has arisen because no extant legislation prevents Google or its competitors from collecting and using this vast amount of data. And, as discussed below, despite its

ongoing efforts to improve, Google appears to do so under the guise of consent few people understand how to disable. Even with consent, it seems clear that most Google users do not know how the consent flow to control their collection of data works, nor do they know Google is logging their location 240 times a day. It is not within this Court's purview to decide such issues, but it urges legislative action. Thoughtful legislation could not only protect the privacy of citizens, but also could relieve companies of the burden to police law enforcement requests for the data they lawfully have.

B. Because the Government Lacked Particularized Probable Cause as to Every Google User in the Geofence, the Warrant Violates the Fourth Amendment

At base, this particular Geofence Warrant is invalid. The Fourth Circuit has clearly articulated that warrants, like this one, that authorize the search of every person within a particular area must establish probable cause to search every one of those persons. Here, however, the warrant lacked any semblance of such particularized probable cause to search each of its nineteen targets, and the magistrate thus lacked a substantial basis to conclude that the requisite probable cause existed. And to the extent the Government would argue that Steps 2 and 3 cure the warrant's defects as to probable cause, such an argument is unavailing here. The Government itself contends that law enforcement demonstrated probable cause to obtain *all* the data sought without any narrowing measures (*i.e.*, de-anonymized and geographically unlimited data from everyone within the geofence). In any event, Steps 2 and 3—undertaken with

no judicial review whatsoever—improperly provided law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions. These steps therefore cannot buttress the rest of the warrant, as they fail independently under the Fourth Amendment's particularity prong.

1. Legal Standard: The Warrant Requirement

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Stated another way, the Fourth Amendment requires that a warrant (1) be supported by probable cause; (2) particularly describe the place to be searched and the things to be seized; and, (3) be issued by a neutral, disinterested magistrate.[31] *Dalia v. United States*, 441 U.S. 238, 255, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979) (internal quotations and citations omitted). If a warrant is invalid, the proper remedy in a criminal action is "ordinarily" to suppress the evidence derived from it. *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018).

a. Probable Cause

Whether probable cause for a search exists is a "practical, common-sense" question, asking whether "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v.*

[31] Because this third prong intersects with the Court's good faith analysis, the Court discusses it more fully in Part III.C.2, *infra*.

Gates, 462 U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). It requires only "the kind of fair probability on which reasonable and prudent people, not legal technicians," would rely. *United States v. Jones*, 952 F.3d 153, 158 (4th Cir. 2020) (citing *Florida v. Harris*, 568 U.S. 237, 244, 133 S.Ct. 1050, 185 L.Ed.2d 61 (2013)). Officers must present sufficient information to the magistrate judge [32] to allow him or her to exercise independent judgment. *Gates*, 462 U.S. at 239, 103 S.Ct. 2317. The magistrate cannot simply ratify the bare conclusions of others. *Id.* "When reviewing the probable cause supporting a warrant, a reviewing court must consider only the information presented to the magistrate who issued the warrant." *United States v. Wilhelm*, 80 F.3d 116, 118 (4th Cir. 1996) (citations omitted). "[T]he duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004).

More specifically, a warrant must be "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006) (quoting *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002)). Indeed, the United States Court of Appeals for the Fourth Circuit has established that warrants that authorize the search of "all persons on [a] premise[s]" must show probable cause "to believe that *all* persons on the premises at the time of the search are involved in the criminal activity." *Owens ex rel. Owens v. Lott*, 372 F.3d

[32] In the federal system, the magistrates who review and sign search warrants are judges who must have law degrees. This is not necessarily the case in state judicial systems.

267, 276 (4th Cir. 2004) (emphasis added) (second alteration in original), *overturned on other grounds by Pearson v. Callahan*, 555 U.S. 223, 129 S. Ct. 808, 172 L.Ed.2d 565 (2009). In other words, these warrants must demonstrate "good reason to suspect or believe that anyone present at the anticipated scene will probably be a participant in the criminal activity." *Owens*, 372 F.3d at 276 (internal quotation marks omitted).

At base, probable cause demands that law enforcement possess "a reasonable ground for belief of guilt ... *particularized* with respect to the person to be searched or seized." *Maryland v. Pringle*, 540 U.S. 366, 124 S. Ct. 795, 800, 157 L.Ed.2d 769 (2003) (emphasis added); *see Ybarra v. Illinois*, 444 U.S. 85, 91, 100 S.Ct. 338, 62 L.Ed.2d 238 (1979) ("Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person.") A "person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra*, 444 U.S. at 91, 100 S.Ct. 338.

b. Particularity

A warrant must also be sufficiently "particular[ ]." *Hurwitz*, 459 F.3d at 470. Thus, a warrant must "confine the executing [officers'] discretion by allowing them to seize only evidence of a particular crime." *United States v. Cobb*, 970 F.3d 319, 328 (4th Cir. 2020), as amended (Aug. 17, 2020) (quoting *United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986)). The warrant must therefore "identif[y] the items to be seized by their relation to designated crimes," and the "description of

the items [must] leave[ ] nothing to the discretion of the officer executing the warrant." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (citation omitted). "So long as the warrant describes the items to be seized with enough specificity that the executing officer is able to distinguish between those items which are to be seized and those that are not ... the particularity standard is met." *United States v. Blakeney*, 949 F.3d 851, 862 (4th Cir. 2020) (internal citations and quotations omitted).[33]

2. The Geofence Warrant Fails to Establish Particularized Probable Cause to Search Every Google User Within the Geofence

Although cloaked by the complexities of novel technology, when stripped of those complexities, this *particular* Geofence Warrant lacks sufficient probable cause. [34] The United States Supreme Court has

---

[33] The Framers included the particularity requirement to "end the practice, abhorred by the colonists, of issuing general warrants," which authorized officers to carry out an "exploratory rummaging in a person's belongings." *United States v. Dargan*, 738 F.3d 643, 647 (4th Cir. 2013) (internal citation and quotations omitted). Such "general warrants" placed "the liberty of every [person] in the hands of every petty officer" and were therefore denounced as "the worst instrument of arbitrary power." *Stanford v. Texas*, 379 U.S. 476, 481, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965).

[34] In considering whether the Geofence Warrant is valid, the Court assumes for the sake of analysis that the Government's collection of data here is a "search." *SeeIn re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 736 (noting that by obtaining a warrant and arguing for the validity of that warrant, "the [G]overnment is treating its proposed capture of information

explained that warrants must establish probable cause that is "particularized with respect to the person to be searched or seized." *Pringle*, 124 S. Ct. at 800. This warrant did no such thing. It first sought location information for *all* Google account owners who entered the geofence over the span of an hour.[35] For those Google accounts, the warrant further sought "contextual data points with points of travel outside of the" Geofence for yet another hour—and those data points retained *no* geographical restriction. (ECF No. 54-1, at 4.) Astoundingly, the Government claims that law enforcement established probable cause to obtain *all* information (Steps 1, 2, and 3) from *all* users within the

---

as a search"). Indeed, this is the position Google advances in its amicus brief.

[35] To be clear, the Court sees individuals from whose accounts the Government obtained data as functional subjects of the search, even though the warrant authorized officers to obtain data only from Google's servers. In the same way that users' devices generate IP address information and typically share that information with a third party, so too do users' phones generate Location History data and share that information with Google. *See, e.g.*, *United States v. Broy*, 209 F. Supp. 3d 1045, 1053 (C.D. Ill. 2016) (treating the defendant's IP address as if it is were defendant's property that he disclosed to a third party).

In other words, regardless of which entity's files the Government looked through, the users ultimately retain at least some joint interest in the location data their phones generate. As discussed in Part III.B.4, *infra*, however, because the Court ultimately finds that Det. Hylton acted in good faith, whether these individuals have an expectation of *privacy* in that data must be decided another day. *Cf, e.g., Broy*, 209 F. Supp. 3d at 1053 (finding no reasonable expectation of privacy because the defendant disclosed his IP address to a third party).

geofence without any narrowing measures.[36] Yet the warrant simply did not include any facts to establish probable cause to collect such broad and intrusive data from each one of these individuals.

Law enforcement attempted to justify the warrant by claiming that such a sweeping search "may [have] tend[ed] to identify potential witnesses and/or suspects." (ECF No. 54-1, at 7.) Even if this Court were to assume that a warrant would be justified on the grounds that a search would yield *witnesses* (some of whom had already been interviewed) instead of perpetrators, the Geofence Warrant is completely devoid of any suggestion that all—or even a substantial number of—the individuals searched had participated in or witnessed the crime. *Cf. Owens*, 372 F.3d at 276. To be sure, a fair probability may have existed that the Geofence Warrant would generate the *suspect's* location information.[37] However, the warrant, on its face, also

---

[36] Instead, it appears that law enforcement implemented narrowing measures in this Warrant at the behest of Google. (*See* ECF No. 202, at 275–76 (discussing "go bys," template documents that outline "specific information that [Google] need[s] in order to process the search warrant").)

[37] For instance, Det. Hylton stated in his affidavit that: (1) surveillance tapes revealed that the suspect used a phone; (2) in the officer's "training and experience, when people act in concert ... they frequently utilize cellular telephones;" (3) Google "provides electronic communication services to subscribers, including email services;" (4) Google "has also developed a proprietary operating system for mobile devices, including cellular phones, known as Android;" and, (5) studies show that "91% of American adults own a cellular phone with 56% being smartphones." (ECF No. 54-1, at 6–7.)

swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny.

Indeed, it is difficult to overstate the breadth of this warrant, particularly in light of the narrowness of the Government's probable cause showing. Law enforcement knew only that the perpetrator "had a cell phone in his right hand and appeared to be speaking with someone on the device." (ECF No. 54-1, at 6.) After the police failed to located the suspect via reviewing camera footage, speaking with witnesses, and pursuing two leads, law enforcement simply drew a circle with a 150-meter radius that encompassed the Bank, the entirety of the Church, and the Church's parking lot. [38] The Government then requested location information for *every device* within that area. *See Carpenter*, 138 S. Ct. 2206, 2216 (2018) (describing cell phone location information as "encyclopedic").

What is more, in one instance, this Geofence Warrant captured location data for a user who may not have been *remotely* close enough to the Bank to participate in or witness the robbery. Because the radius of one of the users' confidence intervals stretched to around 387 meters, the Geofence Warrant might have reported that

---

[38] The Government has made passing references to "several [additional] pieces of evidence" that might have guided the contours of the Geofence Warrant. (*E.g.*, ECF No. 202, at 272.) But neither the warrant nor its supporting affidavit referred to this evidence. It is therefore irrelevant to the validity of the warrant. *SeeGroh v. Ramirez*, 540 U.S. 551, 557–58, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004) (declining to consider material contained in a warrant's *application* where the warrant did not incorporate the application by reference).

user's location data to the Government, notwithstanding the fact that he may have simply been present in any number of nearby locations. For example, that person may have been dining inside the Ruby Tuesday restaurant nearby. The person may have been staying at the Hampton Inn Hotel, just north of the Bank. Or, he or she could have been inside his or her own home in the Genito Glen apartment complex or the nearby senior living facility. He or she may have been moving furniture into the nearby self-storage business. Indeed, the person may have been simply driving along Hull Street or Price Club Boulevard. Yet the Government obtained the person's location data just the same. The Government claims that footage depicting the perpetrator holding a phone to his ear—and nothing else—justified this sweeping warrant. That, however, is simply not "[ ]reasonable." U.S. Const. amend. IV.

To further underscore the breadth of this search, Chatrie's expert Spencer McInvaille pointed out a likely "false positive" from the warrant—"Mr. Blue." Mclnvaille testified that this "false positive" individual may not have ever stepped within the geofence—he may have simply driven "outside of the original geofence" on a nearby road, but could have nonetheless appeared "as if [he] were inside the geofence." (ECF No. 201, at 43–44, 65.) Because Google's location estimate for that person could have been "incorrect," Google may have *thought* the person had stepped foot in the target area. (ECF No. 201, at 43–44.) The Government therefore obtained two hours of unrestricted location data for an

individual who perhaps had only driven within the outer vicinity of the crime scene.[39]

This Geofence Warrant therefore suffers from the same probable cause defect as that at issue in *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020). In that case, the Government sought "to erect three geofences." *Id.* 732. Two encompassed the same location during different timeframes, and the other captured a second location. *Id.* Each geofence lasted for forty-five minutes. *Id.* The court remarked that "the proposed warrant would admittedly capture the device IDs ... for all who entered the geofences, which surround locations as to which there is no reason to believe that anyone – other than the Unknown Subject – entering those locations is involved in the subject offense or in any other crime." *Id.* at 752.

---

[39] The fact that data points obtained during Steps 1 and 2 are anonymized when Google reports them does not completely quell this Court's concerns about the invasiveness of this warrant. Even "anonymized" location data—from innocent people—can reveal astonishing glimpses into individuals' private lives when the Government collects data across even a one or two hour period. As noted above, during the March hearing, McInvaille identified three anonymous accounts captured within the geofence—"Mr. Blue," "Mr. Green," and "Ms. Yellow." (ECF No. 201, at 63–71.)

McInvaille testified that, using two hours of only "anonymized" data obtained through the warrant, he could observe each account's reported location, track each account to his or her home, and pinpoint each account's personal identity using publicly available resources even without any Step 3 information. *See* Herbert B. Dixon Jr., *Your Cell Phone is a Spy!*, Am. Bar Ass'n (July 29, 2020), https://bit.ly/3nRuCVq ("Although user data are anonymized, users' identities can nonetheless be determined by following their movements back to their homes and other places.").

There, just as here, the warrant provided the Government "unlimited discretion to obtain from Google the device IDs ... of anyone whose Google-connected devices traversed the geofences (including their vaguely defined margins of error), based on nothing more than the 'propinquity' of these persons to the Unknown Subject at or near the time" of the criminal activity. *Id.* at 753. As that court (and the Supreme Court in *Ybarra*) recognized—and as this Court now concludes—the Fourth Amendment's probable cause requirement demands more than "mere propinquity" to a crime. *Id.* at 752; *Ybarra*, 444 U.S. at 91, 100 S.Ct. 338.

Despite the Government's reliance on *United States v. McLamb*, that case is inapposite. There, the Fourth Circuit upheld a warrant that allowed law enforcement to obtain identifying information of "any user entering a username and password into" an internet-based dark website where users could download or upload child pornography. *United States v. McLamb*, 880 F.3d 685, 689 (4th Cir. 2018). But there, a user's "mere propinquity" to the website *did* necessarily establish probable cause: any user visiting the site likely participated in the criminal conduct of viewing or sharing child pornography. *Id.* Here, on the other hand, a Google user's proximity to the bank robbery does not necessarily suggest that the user participated in the crime. *McLamb* therefore does not inform this case.[40]

---

[40] But one can readily imagine other instances when one's "mere propinquity" to a location, as in *McLamb*, likely *would* provide probable cause to obtain location data for each individual within a geofence. This would *not* necessarily involve improper use of location data. For example, the FBI appears to have employed

Nor does the Government's reliance on *United States v. James* persuade. The *James* court considered a warrant to collect cell tower information (so-called "tower dumps") to determine whether "a particular cellular phone number (ostensibly held by the robber) could be identified during the timeframes of each of the respective robberies." 2018 WL 6566000, at * 1. Law enforcement sought the cell tower data based on the notion that a cell phone number present at the location and time of all six robberies created sufficient probable cause that the number belonged to the robber. *Id.* Ultimately, the court concluded that "there was a fair probability that data from the cellular towers" would contain identifying information about the perpetrator and that therefore the warrants sufficed to allege probable cause. *Id.* at *4. As another court has noted however, *James* did not account for whether probable cause existed to search through the *other* individuals' location information. *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 751; *see also id.* at 752 (distinguishing another tower dump decision from the geofence context because the court discussing the tower dump "stopped the analysis once the court found probable cause in the 'nexus' between the offense and *all* the requested cell phone records, without analyzing whether probable cause existed to

---

geofence technology to locate participants in the January 6 Capitol riots. Mark Harris, *How a Secret Google Geofence Warrant Helped Catch the Capitol Riot Mob*, Wired (Sept. 30, 2021), https://bit.ly/3HktvWU. In that situation, one's presence within the Capitol *would* perhaps, by itself, provide probable cause that an individual was present without permission and was therefore committing a crime.

obtain all of those records." (quoting *In re Search of Cellular Telephone Towers*, 945 F. Supp. 2d 769 (S.D. Tex. 2013)). *James* therefore stopped short of considering whether "particularized" probable cause existed, and it is precisely that lack of narrowly-tailored probable cause that is fatal to this Geofence Warrant.[41]

The Court cautions that it declines to consider today whether a geofence warrant may *ever* satisfy the Fourth Amendment's strictures. *See In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 361–62 (N.D. Ill. 2020) ("[I]t is nearly impossible to pinpoint a search where only the perpetrator's privacy interests are implicated."). Consider, for example, one of the few other federal court opinions to address a geofence warrant—*In re Search of Information That Is Stored at the Premises Controlled*

---

[41] Throughout this litigation, the parties—and Google—drew or resisted analogies to tower dumps. As explained above, however, the lead tower dump cases like *James* do not persuade this Court. Those decisions either decide that individuals' proximity to certain towers *alone* creates probable cause to search them, or altogether neglect to consider such particularity concerns. *James*, 2018 WL 6566000, at *4; *see also United States v. James*, 3 F.4th 1102, 1106 (8th Cir. 2021) (affirming the district court's adoption of the magistrate judge's original opinion on the same grounds). Indeed, the Eighth Circuit in *James* expressly warned that in holding valid the warrants at issue—which connected a robber to a *series* of crimes—was *not* holding "that it is now fair game to search the records from 'cell phone towers near the location of *every* crime.'" *Id.* at 1106. The Court similarly concludes here that the commission of a single crime—by itself, and with no narrowing measures or guardrails—is not sufficient to search geofence records "near the location of *every* crime." *Id.*

by Google LLC, No. 21sc3217, 2021 WL 6196136 (D.D.C. Dec. 30, 2021) [hereinafter "DDC Opinion"]. There, law enforcement devised a two-step process to narrow the list of individuals whose data they would obtain. *Id.* at *5–6. At Step 1, Google would identify all accounts who entered the geofence within the relevant time periods. *Id.* For each of these accounts, Google would turn over only anonymized data. *Id.*

The Government would then review that data, identify likely suspects based on the "mov[ement]" of the users' devices through the geofence, and, crucially, identify to the *court* the devices the Government believed belonged to the perpetrator. *Id.* The *court* could then, at its discretion, order Google to disclose to the Government personally identifying information for devices that belonged to likely suspects. *Id.* In essence, to obtain a warrant authorizing disclosure of de-anonymized data, the Government was required to demonstrate that location data for a *particular* user or set of users would provide evidence of the crime. And crucially, the warrant left ultimate discretion as to which users' information to disclose to the reviewing court, not to Google or law enforcement.

In certain situations, then, law enforcement likely *could* develop initial probable cause to acquire from Google *only* anonymous data from devices within a narrowly circumscribed geofence at Step 1. *See Hurwitz*, 459 F.3d at 473 (a warrant must be "no broader than the probable cause on which it is based"). From there, officers likely could use that narrow, anonymous information to develop probable cause particularized to specific users. Importantly, officers likely could then present that

particularized information to a magistrate or magistrate judge to acquire successively broader and more invasive information. Although the *instant* warrant is invalid, where law enforcement establishes such narrow, particularized probable cause through a series of steps with a court's authorization in between, a geofence warrant may be constitutional.[42]

At bottom however, particularized probable cause "cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be." *Ybarra*, 444 U.S. at 91, 100 S.Ct. 338. The Court finds unpersuasive the United States' inverted probable cause argument—that law

---

[42] The warrant in the DDC Opinion differed in additional ways. For instance, that warrant appears to have sought only location data that fell *within* the geofence across time periods notably shorter than the geofence at bar. *See* DDC Op. at *12 ("[T]he geofence only provides cell phone user's whereabouts in a single area for a handful of minutes on the days in question, not the sum-total of their daily movements."). Here, by contrast, the Government sought two hours of location data *not* bound within the geofence. *Cf.* DDC Op. *12 ("[T]he warrant does not seek location data for days or even hours to track the whereabouts of the perpetrators, but rather location data that is tailored and specific to the time of the [alleged crimes] only." (second alteration in original) (quotation marks and citation omitted)).

In addition to restricting officers' discretion when selecting which accounts for which to obtain personally identifying information, limiting the pool of data returned to only location points *within* the geofence helps assuage this Court's concerns with respect to particularized probable cause, and, more broadly, concerns that broad swaths of anonymous data can be used to pinpoint numerous individuals' identities.

enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby. In essence, the Government's argument rests on precisely the same "mere propinquity to others" rationale the Supreme Court has already rejected as an appropriate basis for a warrant. *Id.* This warrant therefore cannot stand.

3. This Geofence Warrant's Three-Step Process Does Not Cure Its Defects

To the extent the Government would attempt to argue in the alternative that this warrant's three-step process cures any defects with the warrant's particularized probable cause, such an argument is unavailing.[43] Even if this narrowing process cured any of the warrant's shortcomings as to particularized probable cause, this process cannot independently buttress the warrant for an entirely separate reason: clear lack of particularity. Warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. In other words, "[a] warrant that meets the particularity requirement leaves the executing officer with no discretion as what to seize." *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (citing *Stanford v. Texas*, 379 U.S. 476, 485, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965)). But Steps 2 and 3 of this warrant leave the executing officer with *unbridled* discretion and

---

[43] The Court recognizes that the Government primarily argues that it possessed probable cause to obtain *all* data sought regardless of the three-step process.

lack any semblance of objective criteria to guide how officers would narrow the lists of users.

This warrant, for instance, contains no language objectively identifying *which* accounts for which officers would obtain further identifying information. Nor does the warrant provide objective guardrails by which officers could *determine* which accounts would be subject to further scrutiny. Nor does the warrant even simply limit the *number* of devices for which agents could obtain identifying information. Instead, the warrant provided law enforcement unchecked discretion to seize more intrusive and personal data with each round of requests—without ever needing to return to a neutral and detached magistrate for approval.

The facts here underscore the breadth of discretion law enforcement possessed under this warrant.[44] After receiving anonymized information on the nineteen targeted users at Step 1, Det. Hylton requested the additional location information (Step 2) and subscriber information (Step 3) "for all 19 device numbers produced

---

[44] The facts also raise a concern about how even good faith effort by law enforcement can impinge upon constitutional boundaries through a lack of understanding as to what this warrant actually produces and how it does so. While all performed in good faith—especially given this novel and complex process—Det. Hylton returned the warrant before it was served, improperly requested Step 2 and 3 information simultaneously, failed at first to narrow his request at Step 2, and incorrectly tried to add a Step 4 to the process. While the Google LIS allowed only what was permitted under the warrant (which Det. Hylton did not resist), Fourth Amendment protections should not be left in the hands of a private actor.

in [S]tep 1." (ECF No. 96-2, at ¶ 15.) In response, a Google specialist "called Detective Hylton and explained the issues in the Detective's email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant."[45] (ECF No. 96-2, at ¶ 16.) During that call, "[t]he LIS specialist also explained the importance of [S]tep 2 in narrowing." (ECF No. 96-2, at ¶ 16.) Det. Hylton eventually narrowed his requests. Yet he did not specify to Google why he was choosing these particular users.

Google's insistence on narrowing the list does not render this warrant sufficiently particular. For one thing, this warrant's clear text does not specifically allow Google to limit the group of accounts that would be subject to further scrutiny. (*See* ECF No. 54-1, at 4–5 (noting only that Google "shall produce" further information).) But even if it did, Fourth Amendment discretion must be confined to the signing magistrate, not the executing officers or a third party. *United States v. Chadwick*, 433 U.S. 1, 9, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977) ("The judicial warrant has a significant role to play in that it provides the detached scrutiny of a neutral magistrate ...."), *abrogated on other grounds by California v. Acevedo*, 500 U.S. 565, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991). Stated plainly, Steps 2 and 3 "put[ ] no limit on the [G]overnment's discretion to select the device IDs from which it may then derive identifying subscriber information from among the anonymized list of Google-connected devices that traversed the geofences." *In re Search of Information Stored at Premises Controlled by*

---

[45] Det. Hylton received this remonstration despite having executed three geofence warrants prior to this one.

Google, 481 F. Supp. 3d at 754. These Steps accordingly fail to provide the executing officer with clear standards from which he or she could "reasonably ... ascertain and identify ... the place to be searched [or] the items to be seized." *Blakeney*, 949 F.3d at 861. The Government therefore cannot rely on Steps 2 and 3 to supply this warrant with particularized probable cause, as these steps independently fail under the Fourth Amendment's particularity requirement.

4. The Third-Party Doctrine

Lastly, the Court simply cannot determine whether Chatrie "voluntarily" agreed to disclose his Location History data based on this murky, indeterminate record. But the Court expresses its skepticism about the application of the third-party doctrine to geofence technology. Under this doctrine, "a person [generally] has no legitimate expectation of privacy in information he [or she] voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). However, in *Carpenter v. United States*, the Supreme Court refined this principle and held than an individual *does* possess an expectation of privacy in seven days of cell-site location information collected by a wireless carrier. 138 S. Ct. at 2217 & n.3. Here, the Government argues that Chatrie cannot claim a reasonable expectation of privacy in his Location History data because (1) he "voluntarily disclosed" the information to Google; and, (2) the two hours of location data sought here do not implicate the same privacy concerns as the seven days obtained in *Carpenter*. (ECF No. 41, at 11; *see* ECF No. 41, at 9–13.)

The Court thinks otherwise. Common sense underscores Supreme Court Justice Sonia Sotomayor's observation in *United States v. Jones* about "voluntary" collection of electronic information unbeknownst to the subject of the warrant. As to the third-party doctrine, Justice Sotomayor observed that:

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties [because] [t]his approach is ill suited to the digital age.... I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year.

Jones, 565 U.S. at 417–18, 132 S.Ct. 945 (Sotomayor, J., concurring). At base, the topic is complex. And considering the messiness of the current record as to how and when Chatrie "gave consent," the Court cannot—and need not—reach a firm decision on the issue. But the Court remains unconvinced that the third-party doctrine would render hollow Chatrie's expectation of privacy in his data, even for "just" two hours. Google Location History information—perhaps even more so than the cell-site location information at issue in *Carpenter*—is "detailed, encyclopedic, and effortlessly compiled." *Carpenter*, 138 S. Ct. at 2216; *see id.* at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."). Although, unlike in *Carpenter*, Chatrie

apparently took some affirmative steps to enable location history, those steps likely do not constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day.

This is especially so given the limited and partially hidden warnings provided by Google. In the Google Assistant set-up process, the device likely provided Chatrie a single pop-up screen informing him that "[t]his data may be saved and used in any Google service where [he was] signed in to give [him] more personalized experiences," and that he "can see [his] data, delete it and change [his] settings at account.google.com." (ECF No. 147, at ¶ 7; *see* ECF No. 96-1, at ¶ 7; ECF No. 201, at 102; ECF No. 202, at 21.) However, the consent flow did not detail, for example, how frequently Google would record Chatrie's location (every two to six minutes); the amount of data Location History collects (essentially *all* location information); that even if he "stopped" location tracking it was only "paused," meaning Google retained in its Sensorvault all his past movements; or, how precise Location History can be (*i.e.*, down to twenty or so meters).[46] (ECF No. 201, at 122, 136; ECF No. 202, at 71.)

---

[46] As Google's expert Mario McGriff testified, Location History also allows Google to estimate a device's *elevation*. Thus, if New York City law enforcement obtained a geofence warrant with a roughly 150-meter radius (similar in size to the one at issue here) that encircled the Empire State Building, even if it were not fully precise, the police might be able to obtain location data for many thousands of people.

While the Court recognizes that Google puts forth a consistent effort to ensure its users are informed about its use of their data, a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting "YES, I'M IN" at midnight while setting up Google Assistant, even if some text offered warning along the way. The record here makes plain that these "descriptive texts" are less than pellucid. Although the Court cannot reach a final decision on the issue today based on the current record here, Chatrie likely could not have, in a "meaningful sense, ... voluntarily 'assumed the risk' of turning over a comprehensive dossier of his physical movements" to law enforcement. *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745, 99 S.Ct. 2577); *see id.* at 2217 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

C. Because Det. Hylton Consulted with Government Attorneys in the Face of Novel Technology and Obtained Similar Warrants in the Past, and Because the Warrant Was Not Otherwise "So Facially Deficient," the Good-Faith Exception Applies

Despite the warrant's defects, the Court ultimately cannot find that excluding the instant evidence would serve to deter future improper law enforcement conduct. This is particularly so in light of rapidly advancing technology and lack of judicial guidance on this novel investigatory technique, and where, as here, prosecutors and magistrates approved three similar warrants.

1. Legal Standard

The exclusionary rule "is neither 'a personal constitutional right' nor is it 'designed to redress the injury occasioned by an unconstitutional search.'" *United States v. Manafort*, 323 F. Supp. 3d 795, 805 (E.D. Va. 2018) (quoting *Davis v. United States*, 564 U.S. 229, 236, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011)). Rather, the exclusionary rule "is a prudential doctrine created ... to compel respect for" constitutional rights. *Davis*, 564 U.S. at 236–37, 131 S.Ct. 2419 (2011). "[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *McLamb*, 880 F.3d at 690 (internal quotation marks and citation omitted). Where suppression would not produce deterrent benefits, the exclusionary rule does not apply. *United States v. Leon*, 468 U.S. 897, 909, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).

For that reason, evidence obtained pursuant to a search warrant issued by a neutral magistrate need not be excluded if the officer's reliance on the warrant was "objectively reasonable." *Id.* at 922–23, 104 S.Ct. 3405. Generally, the fact that a neutral magistrate has issued a warrant "suffices to establish" that a law enforcement officer has "acted in good faith in conducting the search." *Id.* at 922, 104 S.Ct. 3405. Therefore, searches carried out pursuant to a warrant "rarely require any deep inquiry into reasonableness." *Id.*

The Fourth Circuit has nonetheless set out four categories of cases in which the good-faith exception will not apply:

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

United States v. Doyle, 650 F.3d 460, 467 (4th Cir. 2011) (internal quotation marks and citations omitted). When considering a motion to suppress the fruits of a novel investigative technique, courts generally decline to hold a warrant "facially deficient where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant." *McLamb*, 880 F.3d at 691. Further, "consultation [with Government attorneys prior to seeking a warrant] is a relevant consideration in determining whether the warrant was facially deficient." *United States v. Matthews*, 12 F.4th 647, 657 (7th Cir. 2021).

2. Because Det. Hylton Relied on the Approval of Prior Warrants in the Face of Novel Technology, the Good-Faith Exception Applies

a. Det. Hylton

Despite the warrant failing under Fourth Amendment scrutiny, the *Leon* good faith exception shields the resulting evidence from suppression. The warrant lacked particularized probable cause, but it was not "*so* lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Leon*, 468 U.S. at 923, 104 S.Ct. 3405 (emphasis added). This is particularly so because "the legality of [this] investigative technique [was] unclear," and Det. Hylton sought "advice from counsel before applying for the warrant." *McLamb*, 880 F.3d at 691. When Det. Hylton applied for the Geofence Warrant, no court had yet ruled on the legality of such a technique. And as this Court's preceding analysis demonstrates, the permissibility of geofence warrants is a complex topic, requiring a detailed, nuanced understanding and application of Fourth Amendment principles, which police officers are not and cannot be expected to possess. *See* Part III.B.2, *supra*.[47]

In the face of this legal uncertainty, Det. Hylton relied on his past experience seeking geofence warrants—he had sought three before applying for this one.

---

[47] The Court therefore rejects Chatrie's argument that "one who had even a rudimentary understanding of the Fourth Amendment's particularity and breadth requirements" would know that this warrant was insufficient. (ECF No. 205, at 42.)

Magistrates and prosecutors had approved all three. *See Matthews*, 12 F.4th at 656 (noting the "general principle that attorney involvement supports a finding of good faith"). Det. Hylton testified that these prior warrants were "mostly similar" to the one at bar—all but one incorporated a roughly 150-meter radius, although a "few of them had more locations because of the more robberies to investigate." (ECF No. 202, at 328.) Even accounting for his miscues, in light of the complexities of this case, Det. Hylton's prior acquisition of three similar warrants, and his consultation with Government attorneys before obtaining those warrants, the Court cannot say that Det. Hylton's reliance on the instant warrant was objectively unreasonable. *See McLamb*, 880 F.3d at 691. While magistrate approval and consultation with the prosecution alone cannot and should not mechanically trigger the good-faith exception, exclusion here likely would not "meaningfully deter" improper law enforcement conduct. *Herring v. United States*, 555 U.S. 135, 144, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009).[48]

b. Magistrate Bishop

Nor can this Court conclude that Magistrate Bishop wholly abandoned his role as a detached magistrate as Chatrie argues. *See Doyle*, 650 F.3d at 470. This exception to good faith primarily looks to whether the magistrate "overstep[ped] his [or her] judicial responsibilities and compromise[d] his judicial

[48] This is particularly so because Det. Hylton's "consultation with [G]ovemment attorneys [in the face of untested investigatory techniques] is precisely what *Leon's* 'good faith' expects of law enforcement." *McLamb*, 880 F.3d at 691.

neutrality," *United States v. Gary*, 420 F. Supp. 2d 470, 486 (E.D. Va. 2006) (quoting *United States v. Servance*, 394 F.3d 222, 231 (4th Cir. 2005), *vacated on other grounds by Servance v. United States*, 544 U.S. 1047, 125 S.Ct. 2308, 161 L.Ed.2d 1086 (2005)), by, for example, actively participating in an investigation, *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 327, 99 S.Ct. 2319, 60 L.Ed.2d 920 (1979); retaining a pecuniary interest in issuing the warrant, *Connally v. Georgia*, 429 U.S. 245, 249–51, 97 S.Ct. 546, 50 L.Ed.2d 444 (1977) (per curiam); "rubber stamp[ing]" a warrant that contained a "bare bones" affidavit, *Wilhelm*, 80 F.3d at 121 (4th Cir. 1996); or, failing to make an independent assessment as to the validity of the warrant, *United States v. McKneely*, 810 F. Supp. 1537, 1547 (D. Utah 1993), *rev'd on other grounds by United States v. McKneely*, 6 F.3d 1447 (10th Cir. 1993).

Chatrie has, perhaps, shown that Magistrate Bishop *should have* considered the implications of the Warrant more carefully. But ultimately, he has "produced no evidence to show that the magistrate did not read the affidavit or that he read it so cursorily as to have wholly abandoned his neutral and detached role." *Gary*, 420 F. Supp. 2d at 487; (*see* ECF No. 202, at 361-62 (noting that the magistrate reviewed the warrant for around fifteen or thirty minutes).) Nor did he "suggest that the magistrate acted in a partisan manner or aligned himself with the police. Consequently, ... the second *[Leon* exception] does not bar application of the good-faith exception." *Gary*, 420 F. Supp. 2d at 487. Chatrie further argues that "[t]he magistrate's utter lack of concern regarding the obvious flaws in the warrant constituted a complete abandonment of his role as ... neutral arbiter."

(ECF No. 205, at 41.) But the Fourth Circuit has instructed that such "an allegation that a search warrant application contained grossly insufficient information is best analyzed under the third *Leon* exception." *United States v. Wellman*, 663 F.3d 224, 229 (4th Cir. 2011). And for the reasons explained above, that exception does not warrant suppression either.

Finally, the Court must address Chatrie's challenge to Magistrate Bishop's qualifications. Chatrie contends that Magistrate Bishop did not possess the requisite statutory qualifications to make the instant probable cause determination. The Court first observes that, in Virginia, any United States citizen who is a resident of the Commonwealth is eligible to be appointed as a magistrate with certain limitations not relevant here. Va. Code § 19.2-37. To qualify today, a magistrate need only have "a bachelor's degree from an accredited institution of higher education." Va. Code § 19.2-37(B). And "[a] person initially appointed as a magistrate prior to July 1, 2008, who continues in office without a break in service is *not* required to have a bachelor's degree from an accredited institution of higher education." Va. Code § 19.2-37(B) (emphasis added). No law degree is required. Indeed, "[n]o person appointed as a magistrate on or after July 1, 2008, *may* engage in the practice of law." Va. Code § 19.2-37(F) (emphasis added).

Magistrate Bishop graduated from Pensacola Christian College with a Bachelor of Science Degree in Criminal Justice in May of 2016. He was appointed as a Virginia magistrate roughly two years later in June 2018, began certification school in July 2018, and was formally appointed and "released for independent service on

October 24, 2018." (ECF No. 156, at ¶ 3.) His nine-month probationary period pursuant to Virginia Code § 19.2-38 ended on March 12, 2019. In other words, Magistrate Bishop had been serving as a non-probationary magistrate just *three months* before he signed this sweeping and powerfully intrusive Geofence Warrant on June 14. And he had graduated from college just three years earlier.

Chatrie does not rest on Magistrate Bishop's lack of a law degree. He instead avers that Magistrate Bishop's undergraduate degree was not sufficiently "accredited" under Virginia law. (ECF No. 135, at 6–9.) As noted, Pensacola Christian College does not appear to be officially licensed in Florida. (*See* Ex. B 24, ECF No. 135-2 ("Pensacola Christian College operates in the state of Florida as an independent institution of higher learning that is exempt from state commission oversight as per Florida statutes.").) Further, it does not appear to be accredited by a regional higher-education accrediting agency. *See, e.g.*, Southern Association of Colleges and Schools Commission on Colleges, *Accredited and Candidate List January 2022* (last visited Mar. 1, 2022), https://bit.ly/3cb3ICF. Yet the Transnational Association of Christian Colleges and Schools ("TRACS")[49] accredited the college in 2013. *Pensacola*

[49] TRACS is a national agency recognized by the Council for Higher Education Accreditation and the United States Department of Education. *CHEA-and USDE-Recognized Accrediting Organizations*, CHEA (last visited Mar. 1, 2022), https://bit.ly/3*o*g0sLw.

Christian College, TRACS (last visited Mar. 1, 2022), https://bit.ly/3C22S5j.

Chatrie contends that the TRACS accreditation means little, as "[t]he most widely respected agencies are regional [accrediting] bodies," while "national accrediting agencies are significantly less prestigious." (ECF No. 135, at 7.) He points out that elsewhere, the Virginia Code and Virginia Administrative Code specify that certain professionals receive degrees accredited by specific agencies (typically distinguishing between regional and national entities), and that professionals with similar levels of expertise are typically required to obtain a degree from a regionally accredited school. *See* Va. Code § 54.1-4400; 18 Va. Admin. Code 115-40-22, 160-40-280. If the Court is to read anything into this, however, it is precisely the opposite conclusion from Chatrie's. The notion that Virginia lawmakers narrow the permissive group of accrediting agencies *elsewhere* merely signals that the lawmakers know how to limit the pool of accrediting bodies but chose not to do so here. *Cf Alexis v. Barr*, 960 F.3d 722, 735 n.1 (5th Cir. 2020) (Dennis, J., dissenting) (noting that where a statute defined a term more specifically in one place but not the other, lawmakers had "intentionally omitted" that more specific definition in the other usage). Under Virginia Code § 19.2-37 then, Magistrate Bishop's degree likely suffices.

To the extent Chatrie also attacks Magistrate Bishop's decision because he "would have had, at most, only a few months of experience evaluating warrant applications on his own when he signed the geofence warrant," that argument cannot prevail given Virginia's statutory

scheme. (ECF No. 135, at 9.) Virginia magistrates must complete a training program, pass a certification examination, and serve a nine-month probationary period before hearing cases without supervision. Va. Code § 19.2-38. Magistrate Bishop had done this, and he had been certified by the Commonwealth of Virginia's Office of Executive Secretary. As a general principle, "[s]tates are entitled to some flexibility and leeway in their designation of magistrates, so long as all are neutral and detached and capable of the probable-cause determination required of them." *Shadwick v. City of Tampa*, 407 U.S. 345, 354, 92 S.Ct. 2119, 32 L.Ed.2d 783 (1972). In the ordinary course then, Virginia sufficiently trains its magistrates to determine probable cause.

Frankly, however, it is not clear to the Court that *any* person just three years out of college should be burdened with the responsibility of approving or rejecting a warrant of this complexity and magnitude. The Court certainly does not impute any bad faith or improper action by Magistrate Bishop (or the Commonwealth). This case has shown, however, the myriad ways that geofencing instigates a massive intrusion into individual rights, and it does so without notice to potentially thousands of persons with phones within it. It seems less than evident that all law enforcement officers have a clear understanding of the invasive scope of these warrants either. Nor do most magistrates, with or without a law degree. Ultimately, it is for the General Assembly to review or change its magistrate practice given this new technology, and one hopes they would.

In any event, even if Magistrate Bishop's degree or lack of experience did not qualify him to make this consequential finding, the good faith exception would still apply. The Fourth Circuit recently concluded in *McLamb* that the good faith exception is not categorically inapplicable even if the instant "warrant ... reache[s] beyond the boundaries of a magistrate judge's jurisdiction" where suppression would not "produce an appreciable deterrence on law enforcement." 880 F.3d at 691 (internal quotation marks omitted). The Court finds that suppression based on a technical defect of the magistrate's credentials would not serve to deter improper law enforcement conduct. In a typical investigation, officers simply cannot be required to consult a magistrate's resume before approaching that magistrate to obtain a warrant.

IV. Conclusion

Despite the Court finding good faith here, the Court nonetheless strongly cautions that this exception may not carry the day in the future. This Court will not simply rubber stamp geofence warrants. If the Government is to continue to employ these warrants, it must take care to establish particularized probable cause. As the legal landscape confronts newly developed technology and further illuminates Fourth Amendment rights in the face of geofence practices, future geofence warrants may require additional efforts to seek court approval in between Steps, or to limit the geographic and temporal information sought. But in light of the complex legal issues that lead to this Court's conclusion, the Court cannot say that Det. Hylton's reliance on the Geofence Warrant was objectively unreasonable.

Accordingly, the *Leon* good faith exception applies, and the Court will deny Chatrie's motion to suppress evidence obtained as a result of the Geofence Warrant.

For the foregoing reasons, the Court will deny the Motion to Suppress. (ECF No. 29.) An appropriate Order shall issue.