

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff/Appellee,

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Remand From the
United States Supreme Court

APPELLANT'S SUPPLEMENTAL APPENDIX

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

GEREMY C. KAMENS
Federal Public Defender

LAURA J. KOENIG
PATRICK L. BRYANT
Assistant Federal Public Defenders
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800
laura_koenig@fd.org
patrick_bryant@fd.org

Counsel for Appellant

SUPPLEMENTAL APPENDIX

Appendix A: *United States v. Chatrue*, 107 F.4th 319 (4th Cir. 2024).....SA 1

Appendix B: *United States v. Chatrue*, 136 F.4th 100 (4th Cir. 2025) (en banc).....SA 56

Appendix C: *Chatrue v. United States*, 609 U.S. ___, 146 S. Ct. 2193 (2026) SA 119

U.S. v. CHATRIE

319

Cite as 107 F.4th 319 (4th Cir. 2024)

enhancement to reach the maximum total offense level of 43, application of the hate-crime enhancement did not affect the outcome of the sentencing proceedings. *See* U.S.S.G. Ch. 5, Pt. A, App. Note 2 (“An offense level of more than 43 is to be treated as an offense level of 43.”). Sherifi admitted as much when he conceded that “[s]tanding alone . . . the district court’s § 3A1.1(a) error may not have affected the outcome of sentencing.” Appellant’s Br. at 39.

Sherifi was also not prejudiced by the hate-crime enhancement because the jury found him guilty of two different conspiracies to commit jihad, and thus necessarily found that he intentionally targeted non-Muslim victims based on their religion. The indictment and the government’s theory of the case relied on the central premise that Sherifi and his co-defendants conspired to “advance violent jihad,” which to them meant “fighting against the kuffar,” a derogatory word for non-Muslims. *Has-san*, 742 F.3d at 112, 116. That was sufficient for the district court to apply the hate-crime enhancement. No part of U.S.S.G. § 3A1.1(a) requires that the jury find the defendant’s discriminatory motivation by special verdict, and we refuse to read such a requirement into the Guidelines. *See In Re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 93, 154 (2d Cir. 2008) (upholding hate-crime enhancement when record showed that jury must have found conspiracy targeted victims based on national origin); *United States v. Pospisil*, 186 F.3d 1023, 1031 (8th Cir. 1999) (rejecting argument that Guidelines require jury to make a “special finding” before the sentencing court applies the hate-crime enhancement).

Nor can Sherifi show that the hate-crime enhancement, even if it was applied without the requisite jury finding, seriously affected the fairness, integrity, or public

reputation of the judicial proceedings. The record is littered with testimony showing that Sherifi wanted to “kill a thousand . . . kuffar,” J.A. 1101, that he thought “anyone who didn’t even believe in the Prophet Mohammad was a legitimate target for jihad,” J.A. 2201, and that he felt it was “obligatory” to attack any “non-Muslims [that] have entered into the Muslim land,” J.A. 2248. Sherifi himself does not contest on appeal that he selected his victims on the basis of their religion. *See* Appellant’s Br. at 37–41. Because the overwhelming and essentially uncontroverted evidence at trial “admits of only one result”—that Sherifi targeted his victims based on their religious beliefs—“there is simply no basis for concluding” that the application of the hate-crime enhancement “seriously affected the fairness, integrity or public reputation of judicial proceedings.” *United States v. Brown*, 757 F.3d 183, 194 (4th Cir. 2014) (internal quotations omitted); *see also Cotton*, 535 U.S. at 633, 122 S.Ct. 1781. We therefore reject Sherifi’s request for resentencing.

III.

For the foregoing reasons, the judgment of the district court is affirmed.

AFFIRMED



**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.

No. 22-4489

United States Court of Appeals,
Fourth Circuit.

Argued: December 8, 2023

Decided: July 9, 2024

Background: After the United States District Court for the Eastern District of Virginia, M. Hannah Lauck, J., 590 F.Supp.3d 901, denied defendant's motion to suppress location data obtained using geofence warrant, defendant pled guilty to forced accompaniment during armed credit union robbery, and using, carrying, or brandishing firearm during and in relation to crime of violence. Defendant appealed.

Holdings: The Court of Appeals, Richardson, Circuit Judge, held that government did not conduct search under Fourth Amendment by obtaining location history data from defendant's mobile device.

Affirmed.

Wynn, Circuit Judge, dissented and filed opinion.

1. Search, Seizure, and Arrest ⇌423, 541

To trigger Fourth Amendment's protections, government must conduct search or seizure covered by Fourth Amendment. U.S. Const. Amend. 4.

2. Search, Seizure, and Arrest ⇌431

For Fourth Amendment purposes, "search" occurs when government invades

individual's reasonable expectation of privacy. U.S. Const. Amend. 4.

See publication Words and Phrases for other judicial constructions and definitions.

3. Search, Seizure, and Arrest ⇌527

Person has no legitimate expectation of privacy protected by Fourth Amendment in information he voluntarily turns over to third parties, even if information is revealed on assumption that it will be used only for limited purpose and confidence placed in third party will not be betrayed. U.S. Const. Amend. 4.

4. Search, Seizure, and Arrest ⇌519

Defendant did not have reasonable expectation of privacy in location history data from his mobile device that law enforcement obtained from technology company pursuant to geofence warrant, and thus government did not conduct search under Fourth Amendment by obtaining it, even though company had looked through its entire location history database at government's behest; government only had access to two hours' worth of defendant's location history data, and defendant had voluntarily exposed his location information to company by opting in to location history setting on device after company had provided ample notice about nature of setting. U.S. Const. Amend. 4.

5. Search, Seizure, and Arrest ⇌457

Government conducts "search" for Fourth Amendment purposes when it uses sense-enhancing technology to learn information from inside private space that it could not have learned without physically intruding on that space. U.S. Const. Amend. 4.

See publication Words and Phrases for other judicial constructions and definitions.

U.S. v. CHATRIE

321

Cite as 107 F.4th 319 (4th Cir. 2024)

6. Search, Seizure, and Arrest ⇨1733

Someone who does not have Fourth Amendment interest in place or thing searched lacks standing to challenge that search. U.S. Const. Amend. 4.

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)

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: Jeremy 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.

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.

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 war-

rant 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 Chatrerie'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 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

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 Chatrerie's information in 2019. We do not opine on how Google's changes will affect future cases.

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

U.S. v. CHATRIE

323

Cite as 107 F.4th 319 (4th Cir. 2024)

“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.

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, in-

cluding 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 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

“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.

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.

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.

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.

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

U.S. v. CHATRIE

325

Cite as 107 F.4th 319 (4th Cir. 2024)

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. Al-

though 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

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

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.

district court “on any grounds apparent from the record”).

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

[1] 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.

[2] 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.

[3] 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

Despite its clear mandate, the third-party doctrine has proved difficult to implement in the digital age. After all, “people

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).

U.S. v. CHATRIE

327

Cite as 107 F.4th 319 (4th Cir. 2024)

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 long-term surveillance differently. *Id.* at 283–84, 103 S.Ct. 1081.¹¹

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

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).

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 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 mo-

12. Although the government requested 7 days’ worth of CSLI from one wireless carrier and 152 days’ worth from the other, it re-

ceived only 2 days’ worth from the former and 127 days’ worth from the latter. *Carpenter*, 585 U.S. at 302, 138 S.Ct. 2206.

U.S. v. CHATRIE

329

Cite as 107 F.4th 319 (4th Cir. 2024)

ment, 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 of around 90% of the city each day.” *Id.* at 334. We interpreted *Carpenter* to “solidify[] 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 pri-

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 govern-

ment’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).

vacy and thereby conducted a search. *Id.* at 346.¹⁴

B. Application

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

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 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 carri-

ers.'" (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.

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).

U.S. v. CHATRIE

331

Cite as 107 F.4th 319 (4th Cir. 2024)

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. 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,

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.

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

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.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 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. 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.

U.S. v. CHATRIE

333

Cite as 107 F.4th 319 (4th Cir. 2024)

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 *voilà!*—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 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.

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

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 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)).

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*, 585 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,

U.S. v. CHATRIE

335

Cite as 107 F.4th 319 (4th Cir. 2024)

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

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 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

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 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.

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.

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 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.

[5,6] 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 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

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 observa-

tion 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.

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 tech-

U.S. v. CHATRIE

337

Cite as 107 F.4th 319 (4th Cir. 2024)

that 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 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 “declin[e]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 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,

nology to peer into a person's curtilage if the person knowingly 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.

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.

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

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 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.”); *Flor-*

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 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.

U.S. v. CHATRIE

339

Cite as 107 F.4th 319 (4th Cir. 2024)

ida 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 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 con-

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.

ducted 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 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. 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

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.

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).

U.S. v. CHATRIE

341

Cite as 107 F.4th 319 (4th Cir. 2024)

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 judg-

U.S. v. CHATRIE

Cite as 107 F.4th 319 (4th Cir. 2024)

343

ment). 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 ordi-

nary 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 princi-

ples 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]lea [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, multi-factor 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.

U.S. v. CHATRIE

345

Cite as 107 F.4th 319 (4th Cir. 2024)

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 circum-

stances” 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 consid-

erations 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) (multi-factor 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 anal-

U.S. v. CHATRIE

347

Cite as 107 F.4th 319 (4th Cir. 2024)

ysis, *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

U.S. v. CHATRIE

349

Cite as 107 F.4th 319 (4th Cir. 2024)

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* decision³—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).

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

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.

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 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 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 Chatrīe’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.

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 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.

6. I note that it is unclear from the record whether the geofence intrusion indeed reached inside Chatrīe’s home or his constitutionally protected spaces.

U.S. v. CHATRIE

351

Cite as 107 F.4th 319 (4th Cir. 2024)

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.

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” wheth-

er 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, encycloped-

ic, 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.

U.S. v. CHATRIE

353

Cite as 107 F.4th 319 (4th Cir. 2024)

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 personal-

ly. *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

U.S. v. CHATRIE

355

Cite as 107 F.4th 319 (4th Cir. 2024)

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 Chatrle'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

U.S. v. CHATRIE

357

Cite as 107 F.4th 319 (4th Cir. 2024)

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 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

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.

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 month-

ly 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, 138 S.Ct.

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 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.

U.S. v. CHATRIE

359

Cite as 107 F.4th 319 (4th Cir. 2024)

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 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.”).

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/54-V5-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

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.

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 reason-

able expectation of privacy in that information. 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, disintegrated 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.

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 con-

sumer-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.

U.S. v. CHATRIE

361

Cite as 107 F.4th 319 (4th Cir. 2024)

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 Chatrue’s Location History data constituted a Fourth Amendment search.¹²

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. *Chatrue*, 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

U.S. v. CHATRIE

363

Cite as 107 F.4th 319 (4th Cir. 2024)

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 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[ie]d 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 de-

clares 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.

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.

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 enforce-

U.S. v. CHATRIE

365

Cite as 107 F.4th 319 (4th Cir. 2024)

ment 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—“voilà!”—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,”

U.S. v. CHATRIE

367

Cite as 107 F.4th 319 (4th Cir. 2024)

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

U.S. v. CHATRIE

369

Cite as 107 F.4th 319 (4th Cir. 2024)

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

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.

has long drawn a line between public and private spaces—concluding that 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

U.S. v. CHATRIE

371

Cite as 107 F.4th 319 (4th Cir. 2024)

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.

c.

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

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) [https://perma.cc/27JX-ANVC].

U.S. v. NKONGHO

373

Cite as 107 F.4th 373 (4th Cir. 2024)

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 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.



UNITED STATES of America,
Plaintiff – Appellee,

v.

Eunice Bisong NKONGHO,
Defendant – Appellant.

No. 22-4261

United States Court of Appeals,
Fourth Circuit.

Argued: December 6, 2023

Decided: July 10, 2024

Background: Following denial of motion to suppress, 2021 WL 4421883, defendant was convicted in the United States District Court for the District of Maryland, George J. Hazel, J., of money laundering and con-

garded.” Fed. R. Crim. P. 52(a). Accordingly, the judgment of the district court in accepting Brown’s guilty plea and in sentencing him to 180 months’ imprisonment, as enhanced by ACCA, is affirmed.

AFFIRMED



**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.

No. 22-4489

United States Court of Appeals,
Fourth Circuit.

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)

ARGUED: Michael William Price, NATIONAL ASSOCIATION OF CRIMI-

NAL DEFENSE LAWYERS, Washington, D.C., for Appellant. Nathan Paul Judish, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellee. ON BRIEF: Jeremy 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

U.S. v. CHATRIE

101

Cite as 136 F.4th 100 (4th Cir. 2025)

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.

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.

ON REHEARING EN BANC

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

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 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

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 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.

U.S. v. CHATRIE

103

Cite as 136 F.4th 100 (4th Cir. 2025)

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 time-frame 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, 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

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.

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

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

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 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.

U.S. v. CHATRIE

105

Cite as 136 F.4th 100 (4th Cir. 2025)

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 “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 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, hamstringing 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

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 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 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>].

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

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

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.”).

U.S. v. CHATRIE

107

Cite as 136 F.4th 100 (4th Cir. 2025)

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.

Without any directly governing case law, Hylton understandably relied on the previ-

ous 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

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.

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

U.S. v. CHATRIE

109

Cite as 136 F.4th 100 (4th Cir. 2025)

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 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).

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.

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

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].

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.

U.S. v. CHATRIE

111

Cite as 136 F.4th 100 (4th Cir. 2025)

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 lia-

bility 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.

U.S. v. CHATRIE

Cite as 136 F.4th 100 (4th Cir. 2025)

113

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 move-

ments” — 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).

U.S. v. CHATRIE

115

Cite as 136 F.4th 100 (4th Cir. 2025)

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. amend. IV. Surveillance technologies, though also deployed in the name of security, pose a dynamic and resilient threat to that right.

1. Although I believe that this case involved a Fourth Amendment search—and that we should say so—I acknowledge that the condi-

tions for application of the good-faith exception to the exclusionary rule are met here.

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

U.S. v. CHATRIE

117

Cite as 136 F.4th 100 (4th Cir. 2025)

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 [] preser-

vation 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

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 advance-

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

U.S. v. CHATRIE

119

Cite as 136 F.4th 100 (4th Cir. 2025)

ments 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 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 con-

cluded 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 *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

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”).

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. 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*

U.S. v. CHATRIE

121

Cite as 136 F.4th 100 (4th Cir. 2025)

application of the *Carpenter* factors in 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 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 re-

corded 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

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.

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.

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.

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

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

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., 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

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.

U.S. v. CHATRIE

123

Cite as 136 F.4th 100 (4th Cir. 2025)

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

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 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;

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 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.”).

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.

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 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).

U.S. v. CHATRIE

125

Cite as 136 F.4th 100 (4th Cir. 2025)

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

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 Cata-*

lyst 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

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 “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

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).

12. Although the CSLI data at issue in *Carpenter* was only collected at the start and end of

U.S. v. CHATRIE

127

Cite as 136 F.4th 100 (4th Cir. 2025)

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.

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.

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

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 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).

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)).

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

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."

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

Through that single tap, Location History is enabled. *See id.*

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

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.

U.S. v. CHATRIE

129

Cite as 136 F.4th 100 (4th Cir. 2025)

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

* * *

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 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 Lo-

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 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 be-

fore 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.

cation 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 undoubt-

edly 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.

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

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 investiga-

tory 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>].

U.S. v. CHATRIE

131

Cite as 136 F.4th 100 (4th Cir. 2025)

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

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 bene-

fits 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

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.

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.

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.

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.

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.

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 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

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.

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.

U.S. v. CHATRIE

133

Cite as 136 F.4th 100 (4th Cir. 2025)

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, 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

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.

U.S. v. CHATRIE

135

Cite as 136 F.4th 100 (4th Cir. 2025)

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

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).

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 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

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 tres-

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).

U.S. v. CHATRIE

137

Cite as 136 F.4th 100 (4th Cir. 2025)

pass. The Court eventually considered this issue in *Carpenter*. *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. 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, 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

12. Although the government requested 7 days’ worth of CSLI from one wireless carrier and 152 days’ worth from the other, it re-

ceived only 2 days’ worth from the former and 127 days’ worth from the latter. *Carpenter*, 585 U.S. at 302, 138 S.Ct. 2206.

‘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 inter-

preted *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. *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

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 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).

U.S. v. CHATRIE

Cite as 136 F.4th 100 (4th Cir. 2025)

139

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 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 *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.

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 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, 133–34, 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).

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 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 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,

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.

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

U.S. v. CHATRIE

141

Cite as 136 F.4th 100 (4th Cir. 2025)

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

* * *

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.

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 dis-

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 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.

strict 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 exclu-

sion 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 Of-

U.S. v. CHATRIE

143

Cite as 136 F.4th 100 (4th Cir. 2025)

fice 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 cell-phones 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 pseudonymized¹ Google 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

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

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.

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 ex-

pectation 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

U.S. v. CHATRIE

145

Cite as 136 F.4th 100 (4th Cir. 2025)

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 Govern-

ment 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 evalu-

ating 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 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.*

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).

U.S. v. CHATRIE

147

Cite as 136 F.4th 100 (4th Cir. 2025)

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 tele-

communications 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 ex-

haustive 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 third³ requests to Google. These re-

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* re-

quested 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.

U.S. v. CHATRIE

149

Cite as 136 F.4th 100 (4th Cir. 2025)

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

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

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 anon-

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

ymous 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 Chatrue 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 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

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.

U.S. v. CHATRIE

151

Cite as 136 F.4th 100 (4th Cir. 2025)

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 policies 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 collect-

U.S. v. CHATRIE

153

Cite as 136 F.4th 100 (4th Cir. 2025)

ed. 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. LaFare, *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 consti-

tutional 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 Loca-

tion 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-

U.S. v. CHATRIE

155

Cite as 136 F.4th 100 (4th Cir. 2025)

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 data-

base, 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, 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

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.

U.S. v. CHATRIE

157

Cite as 136 F.4th 100 (4th Cir. 2025)

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 Amend-

ment. 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

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”).

the list of users at Steps Two 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,

U.S. v. CHATRIE

159

Cite as 136 F.4th 100 (4th Cir. 2025)

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 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 indiscre-

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”).

tions. 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.

U.S. v. CHATRIE

161

Cite as 136 F.4th 100 (4th Cir. 2025)

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 coun-

sel, 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 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.



UNITED STATES of America,
Plaintiff – Appellee,

v.

Raymond DUGAN, Defendant –
Appellant.

No. 22-4642

United States Court of Appeals,
Fourth Circuit.

Argued: December 11, 2024

Decided: May 1, 2025

Background: After his motions to compel discovery and to suppress evidence seized pursuant to search warrant were denied, defendant was convicted in the United States District Court for the Southern District of West Virginia, Joseph R. Goodwin, J., of accessing with intent to view child pornography and was sentenced to 54

months' imprisonment followed by five years of supervised release, and was ordered to pay a total of \$22,000 in restitution. Defendant appealed.

Holdings: The Court of Appeals, King, Circuit Judge, held that:

- (1) defendant's speculations did support motion to compel discovery of foreign agency's investigative techniques and cooperation under *Brady*;
- (2) district court did not abuse its discretion in denying defendant's motion to compel evidence;
- (3) facts recounted in search warrant affidavit gave magistrate judge a substantial basis for finding probable cause to issue search warrant; and
- (4) district court properly exercised its discretion in ordering defendant to pay restitution to child victims in amounts exceeding statutory minimum of \$3,000 per victim.

Affirmed.

1. Criminal Law $\S$ 1139

In absence of factual findings, Court of Appeals reviews de novo district court's denial of motion to compel, brought under *Brady*.

2. Criminal Law $\S$ 1148

Court of Appeals reviews for abuse of discretion district court's denial of motion to compel discovery. Fed. R. Crim. P. 16(a)(1)(E).

3. Criminal Law $\S$ 1139, 1158.12

In assessing denial of motion to suppress, Court of Appeals reviews district court's legal conclusions de novo and its factual findings for clear error.

4. Criminal Law $\S$ 1134.35

In assessing probable cause determination by magistrate judge asked to issue a search warrant, Court of Appeals applies

146 S.Ct. 2193

Supreme Court of the United States.

Okello T. CHATRIE, Petitioner

v.

UNITED STATES

No. 25–112

|

Argued April 27, 2026

|

Decided June 29, 2026

Synopsis

Background: Following denial of motion to suppress evidence obtained from geofence warrant, 590 F.Supp.3d 901, defendant entered conditional guilty plea in the United States District Court for the Eastern District of Virginia. M. Hannah Lauck, Chief Judge, to forced accompaniment during armed credit union robbery and using, carrying, or brandishing firearm during and in relation to crime of violence. Defendant appealed. The United States Court of Appeals for the Fourth Circuit, Richardson, Circuit Judge, 107 F.4th 319, affirmed, and on rehearing en banc, 136 F.4th 100, affirmed. Certiorari was granted.

The Supreme Court, Justice Kagan, held that an individual has a reasonable expectation of privacy in records about his cell phone's location, and police intrude on that constitutionally protected interest, and thus conduct a search, when they demand the information—even though for only a limited time, and from a third-party tech company.

Vacated and remanded.

Chief Justice Roberts and Justices Sotomayor, Kavanaugh, and Jackson joined.

Justice Jackson filed a concurring opinion, in which Justice Sotomayor joined.

Justice Gorsuch filed an opinion concurring in the judgment.

Justice Alito filed a dissenting opinion, in which Justice Thomas joined as to Part I, and in which Justice Barrett joined as to Parts II–B, II–C–1, and II–C–2.

Justice Barrett filed a dissenting opinion.

Procedural Posture(s): Appellate Review; Pre-Trial Hearing Motion.

*Syllabus**

On May 20, 2019, a man robbed a credit union in Midlothian, Virginia. Local police officers learned from witness interviews and surveillance footage that the robber had approached the credit union from a corner of an adjacent church while appearing to talk on a cell phone, but they could not find out anything more, and the robber remained at large. On June 14, the police officers applied to a Virginia magistrate for a geofence warrant directed to Google, which would require Google to hand over data about the cell phones located within a 150-meter radius of the credit union—the so-called “geofence”—near the time of the crime. The application described the cell-phone location data Google collects through a service called Location History, which records the location of a user's cell phone every two minutes or so. The application also explained how that cell-phone location data could help identify the robber, possible accomplices, or additional witnesses. The warrant described a three-step process that the police would follow: at step one, Google would produce anonymized location data for all cell phones within the geofence 30 minutes before to 30 minutes after the robbery; at step two, officers would attempt to narrow the list, and Google would provide additional anonymized data for that narrowed list, consisting of cell-phone locations both inside and outside the geofence during a two-hour period surrounding the robbery; and at step three, officers would further narrow the list, and Google would turn over identifying information, including names and phone numbers, for users on the final list. The magistrate issued the warrant, and through this process, Google ultimately produced three cell-phone users’ identifying information, including petitioner Okello Chatrrie, whose location data showed that he entered the geofence about ten minutes before the robbery and headed toward a residential area immediately after leaving the bank.

Following further police work, a federal grand jury charged Chatrrie with robbery and related firearms offenses, and he moved to suppress the information the police obtained from Google. According to Chatrrie, the officers had acquired that data through a Fourth Amendment search, and the warrant ostensibly authorizing that search was invalid. The District

Court found that the geofence warrant “plainly violates the rights enshrined in [the Fourth] Amendment” but denied the motion based on the good-faith exception to the exclusionary rule. 590 F.Supp.3d 901, 905, 937–938. A divided panel of the Fourth Circuit affirmed on different reasoning, holding that no search occurred because Chatrie “did not have a reasonable expectation of privacy in two hours’ worth of Location History data voluntarily exposed to Google.” 107 F.4th 319, 325. The Fourth Circuit granted rehearing en banc and affirmed in a one-sentence *per curiam*, with the court dividing evenly on whether a Fourth Amendment search had occurred. This Court granted certiorari solely on the question whether the police violated the Fourth Amendment in obtaining Chatrie’s location data.

Held: Police officers conducted a Fourth Amendment search when they acquired Chatrie’s location data from Google because an individual has a reasonable expectation of privacy in his cell-phone location information. Pp. 2204 - 2217.

(a) The Fourth Amendment protects individuals’ reasonable expectations of privacy, and governmental “intrusion into that private sphere generally qualifies as a search.” *Carpenter v. United States*, 585 U.S. 296, 304, 138 S.Ct. 2206, 201 L.Ed.2d 507. The Amendment’s “basic purpose” is “to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials,” *id.*, at 303, 138 S.Ct. 2206, and it was designed “to place obstacles in the way of a too permeating police surveillance,” *United States v. Di Re*, 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210. Pp. 2204 - 2215.

(1) In *Carpenter*, this Court held that accessing cell-site location information (CSLI) constitutes a Fourth Amendment search because “individuals have a reasonable expectation of privacy in the whole of their physical movements,” 585 U.S., at 310, 138 S.Ct. 2206. The Court reasoned that CSLI provides a “detailed” and “encyclopedic” portrait of a person’s whereabouts, *id.*, at 309, 138 S.Ct. 2206, and, with that, “an intimate window into a person’s life,” *id.*, at 311, 138 S.Ct. 2206. Because people “compulsively carry” their cell phones “all the time,” the Court explained, a cell phone “tracks nearly exactly the movements of its owner,” and thus “faithfully follows” him not only through “public thoroughfares [but] into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *Ibid.* The Court further observed that the “newfound tracking capacity” that CSLI gives the police “runs against everyone”—not just those “under investigation”—and “travel[s] back in time,” making possible

a form of surveillance that would have been unknown prior to the digital age, *id.*, at 311–312, 138 S.Ct. 2206. *Carpenter* accordingly held that “[a]llowing government access to cell-site records contravenes” expectations of privacy. *Id.*, at 311, 138 S.Ct. 2206. Pp. 2205 - 2207.

(2) Everything *Carpenter* relied on to find that law enforcement officers conducted a Fourth Amendment search when they accessed CSLI records applies as well or better to the police’s accessing of Location History data. First, Location History provides an even more fine-tuned picture of a person’s movements, pinpointing location within around twenty meters rather than within sectors of one-eighth to four square miles; it records location every two minutes or so for a daily average of 720 chartings rather than 101; and it can estimate elevation to reveal which floor of a building a phone is on. Second, Location History allows police to reconstruct “retrospective[ly],” and with no real effort, people’s comings and goings in any area, enabling “tireless and absolute surveillance” of any number of people in any number of places. *Carpenter*, 585 U.S., at 312, 138 S.Ct. 2206. And third, Location History implicates personal privacy interests even more than CSLI, because Location History is more the cell-phone user’s own. Most cell-phone users have no awareness of CSLI records, and would never try to retrieve them; by contrast, Google users regularly employ Location History as a personal journal. In that way, Location History resembles other private materials—*e.g.*, emails, documents, photographs, or calendars—that even if stored on Google’s servers, a user reasonably views as his own and expects to be shielded from the “inquisitive eyes” of the government. *Id.*, at 305, 138 S.Ct. 2206. Pp. 2207 - 2209.

(3) The Government’s argument that accessing only a short amount of cell-phone location information does not count as a Fourth Amendment search fails. “[E]ven short-term monitoring” can provide “a wealth of detail about [a person’s] familial, political, professional, religious, and sexual associations,” *United States v. Jones*, 565 U.S. 400, 415, 132 S.Ct. 945, 181 L.Ed.2d 911, and this Court has never understood Fourth Amendment protections as kicking in only once an intrusion “goes too far,” *Pennsylvania Coal Co. v. Mahon*, 260 U.S. 393, 415, 43 S.Ct. 158, 67 L.Ed. 322. Where the Fourth Amendment applies, it applies regardless of “the quality or quantity of information” the government obtains. *Kyllo v. United States*, 533 U.S. 27, 37, 121 S.Ct. 2038, 150 L.Ed.2d 94. That approach makes all the more sense when, as with Location History, law enforcement officials can

select the time-limited set of materials they want from an all-encompassing database. Pp. 2208 - 2212.

(4) The Government argues that the so-called third-party doctrine precludes Chatrle from invoking the Fourth Amendment's protections. The idea is that in "authoriz[ing] Google to collect, retain, and use" his location information, Chatrle lost his legitimate expectation of privacy, and therefore his right to complain of a search. Brief for United States 15. But *Carpenter* refused to apply the third-party doctrine to CSLI, and no good reason exists to reach a different result for Location History. In *Carpenter*, the Court rejected application of the third-party doctrine to CSLI because such information is "qualitatively different" from "telephone numbers and bank records," 585 U.S., at 309, 138 S.Ct. 2206—it is incomparably "revealing" and is "not truly 'shared' as one normally understands the term" given that cell phones are "indispensable to participation in modern society," *id.*, at 315, 138 S.Ct. 2206. Both differentiating features apply equally or better to Location History, which is even more "revealing" than CSLI and is "not truly shared" in the normal sense of wanting a third party to see or use it. *Id.*, at 315, 138 S.Ct. 2206. The exposure of that information to Google is merely what happens when a user avails himself of one of the services on his cell phone. The Government's argument that generating Location History, unlike producing CSLI, is a voluntary choice is meritless. That argument ignores how and why Google users turn on Location History: Google repeatedly prompts users to turn on the service, often warning that devices will not "work correctly" otherwise, 2 App. 140–141, while not disclosing in that prompt how frequently users' location information would be recorded, how precise it would be, or how it might be given to the government. More generally, an app-by-app, feature-by-feature method of granting Fourth Amendment protection misapprehends the nature of modern cell-phone use, where nearly everything requires some kind of "affirmative act" beyond "powering up" a given app or service. The Government wishes to disconnect the activities people do on their cell phones from the mere act of carrying a turned-on cell phone (the thing that generates CSLI), with only the latter receiving assured Fourth Amendment protection. But the point of carrying smartphones is to use what is on them—as *Carpenter* said, to use the apps and "services they provide." 585 U.S., at 315, 138 S.Ct. 2206. Accordingly, a cell-phone user is not to be viewed as sharing private information with third parties—which then can be freely passed on to the government—just by doing the ordinary things cell-phone users do. Pp. 2212 - 2215.

(b) The conclusion that a Fourth Amendment search occurred does not resolve this case, because the Fourth Amendment prohibits only searches that are "unreasonable." When law enforcement officials undertake a search to discover evidence of a crime, the reasonableness standard generally requires that they seek a warrant from "a neutral and detached magistrate," *Johnson v. United States*, 333 U.S. 10, 14, 68 S.Ct. 367, 92 L.Ed. 436, who may issue a warrant only when "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. The warrant issued here, as described earlier, was an uncommon, multi-step one, and the parties have contested the legality of each stage of the search process it authorized. The Fourth Circuit did not address the questions that unusual warrant raises. Because this is "a court of review, not of first view," *Cutter v. Wilkinson*, 544 U.S. 709, 718, n. 7, 125 S.Ct. 2113, 161 L.Ed.2d 1020, the Court leaves it up to the Court of Appeals to decide whether, at each step of the search process, the warrant satisfied the Fourth Amendment's requirements of particularity and probable cause. Pp. 2215 - 2217.

136 F.4th 100, vacated and remanded.

KAGAN, J., delivered the opinion of the Court, in which ROBERTS, C. J., and SOTOMAYOR, KAVANAUGH, and JACKSON, JJ., joined. JACKSON, J., filed a concurring opinion, in which SOTOMAYOR, J., joined. GORSUCH, J., filed an opinion concurring in the judgment. ALITO, J., filed a dissenting opinion, in which THOMAS, J., joined as to Part I, and in which BARRETT, J., joined as to Parts II–B, II–C–1, and II–C–2. BARRETT, J., filed a dissenting opinion.

Attorneys and Law Firms

Jeremy C. Kamens, Federal Public Defender, Laura J. Koenig, Patrick L. Bryant, Assistant Federal Public Defenders, Office of the Federal Public Defender, Eastern District of Virginia, Alexandria, VA, Michael W. Price, National Association of Criminal Defense Lawyers, Fourth Amendment Center, Washington, DC, Adam G. Unikowsky, Counsel of Record, Laurel A. Raymond, Anne S. Warnke, Jenner & Block LLP, Washington, DC, David A. Strauss, Sarah M. Konsky, Jenner & Block, Supreme Court and Appellate Clinic at the University of Chicago Law School, Chicago, IL, for Petitioner.

D. John Sauer, Solicitor General, Counsel of Record, A. Tysen Duva, Assistant Attorney General, Eric J. Feigin,

Deputy Solicitor General, Zoe A. Jacoby, Assistant to the Solicitor General, Ethan A. Sachs, Attorney, Department of Justice, Washington, DC, for Respondent.

Opinion

Justice KAGAN delivered the opinion of the Court.

***2199** In recent years, law enforcement officers have employed so-called geofence warrants to obtain information that technology companies collect about their users' cell-phone locations. Suppose that investigators know a crime was committed at a particular place and time, but do not have a suspect. They may draw a "geofence"—a virtual perimeter—around the crime scene and get a warrant compelling a company to hand over data about the cell phones located in that area near the time of the crime. Following a process specified in the warrant, the company will turn over the cell-phone data and eventually identify by name one or more of the users thus disclosed.

The geofence warrant at issue here was directed to Google, and used to solve a bank robbery. Hundreds of millions of Google users have activated a service called Location History, which records the location of a user's cell phone every two minutes or so. Through a geofence warrant, police officers required Google to turn over Location History data revealing cell phones within the vicinity of a bank at around the time it was robbed. At the end of the multi-step process described in the warrant, Google gave the police three names. The Federal Government soon charged one of the individuals thus identified, petitioner Okello Chatrrie, with committing the crime.

Today, we consider how the Fourth Amendment applies to that use of a geofence warrant. Answering that question in full would mean deciding whether the police conducted a Fourth Amendment "search" when they acquired the cell-phone data leading to Chatrrie's arrest and, if so, whether that search was reasonable given the features of the warrant they employed. We decide the first part of that inquiry today, concluding that the police conducted a search when they gained access to Location History data. An individual has a reasonable expectation of privacy in records about his cell phone's location, and police intrude on that constitutionally protected interest when they demand the information—even though for only a limited time, and from a third-party tech company. We leave to the Court of Appeals the further question whether, given the warrant issued, the search here was reasonable, meaning that each of its steps was ***2200** properly described

with particularity and found to be supported by probable cause.

I

A

Modern cell phones, we observed a dozen years ago, are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 573 U.S. 373, 385, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014). Since then, the percentage of Americans who own smartphones has only increased. Today, more than nine in ten Americans own a smartphone. See W. Bishop, Pew Research Center, Mobile Fact Sheet (Nov. 20, 2025) (91%); compare A. Smith, Pew Research Center, Smartphone Ownership—2013 Update (June 5, 2013) (56%). That means they are likely addicted to apps and other services, many of which collect and store "detailed information about all aspects of a person's life." *Riley*, 573 U.S., at 396, 134 S.Ct. 2473.

Among that information is a single fact most pertinent here: where the user's cell phone is located at a given time. Apps of many kinds rely on that datum. Your maps app wants to help you navigate from Point A (where you are) to Point B (where you are going). Ride-sharing apps of course track your location when you are using them, and often do so even when you are not. Weather apps want to tell you about local conditions. Fast-food apps want to identify the closest burger and pizza joints. Fitness apps want to track your running routes. And so on.

This case concerns a form of cell-phone location data called "Location History," which Google apps collect and store.¹ Location History is what it sounds like—a time-stamped record of every place a cell phone has been. Every two minutes or so, Location History draws from an array of sources to log a cell phone's location. Those sources include nearby Wi-Fi networks, Bluetooth beacons, and cell sites, as well as GPS and IP address information. When combined, the signals tracked can determine a cell phone's location within 20 meters. They can also ascertain a phone's elevation, and thus reveal which floor within a building the phone is on. By all accounts, those features make Location History "the most sweeping, granular, and comprehensive tool" existing today

for collecting and storing location data. 590 F.Supp.3d 901, 907 (ED Va. 2022).

Google repeatedly prompts users to enable Location History, and over 500 million users worldwide have done so. The first prompt comes when a user initially establishes a Google account. If that spur is ignored, another will arrive when a user sets up a Google app—like Google Assistant, Google Maps, or Google Photos—on his phone or other device. Android (though not iPhone) users are specifically warned that their devices will not “work correctly” unless they turn on Location History. 2 App. 140–141. And once a user does so, the service runs—and runs constantly—in the background. Regardless whether the user has a Google app open—or whether he is using his phone at all—Location History remains active. Indeed, it continues to work even if the user deletes the app through which he first turned it on. Location History stops only if a user affirmatively stops it. Sans that intervention, it tracks and *2201 tracks and tracks a user’s cell phone (and other devices).

Google stores all Location History data in the cloud, rather than on a user’s device—though that choice makes no real difference to the user. “Cloud computing” refers to “the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself.” *Riley*, 573 U.S., at 397, 134 S.Ct. 2473. Because it exists, Google can store information on its own servers, while the user can view it as if stored on his cell phone. Such remote storage, we have explained, is common: “Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.” *Ibid.* So, for example, Google usually stores users’ emails, documents, and photographs on company servers instead of on individual devices. See Brief for Google LLC as *Amicus Curiae* 3, 37–38. And the same is true of the information generated by Location History, which is stored in a single central repository on Google’s servers.² That data exists someplace remote, but a user sees it—and the content Google creates from it—in the palm of his hand. The user thus can access a “Timeline” showing where he has traveled when; receive real-time updates about his daily commute; and take advantage of maps and recommendations based on his usual movements.

B

In the last decade, Google’s Location History data has also served another function, though this one unknown to most users: That data, as obtained through a geofence warrant, can enable law enforcement officers to solve hard-to-solve crimes. Such a warrant, as earlier described, seeks information about the cell phones located in the vicinity of a crime scene at around the time the crime was committed. See *supra*, at 2199. The goal, put simply, is to find out who was there and so who might have done it. (There are usually better ways to investigate an already-known suspect—like seeking only his location data.) And the mechanism is to use the offender’s cell phone as an identifying device. The warrant specifies a timeframe and maps an area (with the geofence as its perimeter), and demands information about the cell phones—and their users—present within it. There is some uncertainty about how often the technique in fact works. See Brief for Orin S. Kerr as *Amicus Curiae* 14 (Kerr Brief). But its use among law enforcement officers has flourished. Google received its first geofence warrant in 2016. See 590 F.Supp.3d at 914. Two years later, it received 982; and two years after that, more than 11,000. See Google, Supplemental Information on Geofence Warrants in The United States (Aug. 2021), https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf (archived at <https://perma.cc/LN4P-KQJA>). Though the details vary, each has made the same essential demand: Tell us, through cell-phone location data, who was there when a crime happened.³

*2202 As those demands began to proliferate, Google worked with law enforcement officials to develop a three-step protocol to govern geofence warrants. At the first step, Google produces anonymized (*i.e.*, no names attached) location data for all cell phones (or other devices) within the geofence—typically, a circle with a designated radius surrounding a latitude/longitude coordinate—during

a specified timeframe. That data generally includes each phone's latitude/longitude coordinate and corresponding timestamp; an estimate of that information's accuracy; and a description of the information's source (*e.g.*, a Wi-Fi network, a cell site, or some other). The data at this stage shows each user's location, every two minutes or so, within the geofence. At the second step of the process, officials review the data produced and typically ask Google to provide additional information for a subset of still-anonymized users. That new data is usually for a longer timeframe than first specified; it also shows the user's location outside, as well as inside, the geofence. Finally, at the third step, officials demand the identities of a further subset of users—their names, email addresses, and phone numbers. Thus, the geofence warrant is designed to eventually produce a select number of identified users suspected of committing the crime under investigation.

C

On May 20, 2019, at about 4:50 p.m., a man robbed a credit union in Midlothian, Virginia. The robber presented a teller with a handwritten note demanding \$100,000, threatening to hurt her and her family if she did not comply, and warning her that he had “boys on the lookout out side.” 590 F.Supp.3d at 905–906. When the teller replied that she did not have access to that amount of money, the robber brandished a firearm. He ordered everyone in the bank to the ground, and forced the bank's manager to open a safe and put \$195,000 into a bag. The robber then left on foot with the money.

Local police officers responded to the scene and began an investigation. They learned, from witness interviews and surveillance-camera footage, that the robber had approached the credit union from a corner of an adjacent church, while appearing to talk on a cell phone. But they could not find out anything more, and the robber remained at large.

On June 14, the police officers thus applied to a Virginia magistrate for a geofence warrant directed to Google. The application described the cell-phone location data Google collects, and explained how that data could lead to identifying the robber, his possible accomplices, or additional witnesses to the crime. Success was particularly likely here, the application stated, because the robber appeared to be using his phone when he entered the credit union, and may even have been speaking with an accomplice. The officers' proposed geofence was a circle with a radius of 150 meters surrounding the credit union.

The warrant application went on to describe the three-step process that the police would follow to obtain the location information sought. At step one, Google would produce anonymized location data for all cell phones within the geofence in the hour between 4:20 and 5:20 p.m. (30 minutes before to 30 minutes after the robbery). At step two, police officers would “attempt to narrow down the list [of devices] by reviewing the time stamped location coordinates for each [device] and comparing that against the known time and location information that is specific to this *2203 crime.” 2 App. 136. For that narrowed list, Google would provide additional (but still anonymized) data—cell-phone locations both inside and outside the geofence during a two-hour period (so now from 3:50 to 5:50 p.m.). Finally, at step three, police would again “attempt to narrow down the list by comparing this additional information regarding travel and time against the known time and location information that is specific to this crime.” *Id.*, at 137. And Google would then turn over identifying information for each user on the final list, including his name and phone number.

The magistrate issued the warrant, and officers executed it in the manner prescribed. At the first stage of the process, Google gave up anonymized data for 19 users found within the geofence during the hour within which the robbery occurred. At the second stage, the officers winnowed the list to nine users. And Google produced anonymized data showing their movements both inside and outside the geofence for the extended two-hour period. At the third and last step, the police again narrowed the list, this time to three users. Google responded with their identifying information. One of the three was Chatrie. The location data showed that he entered the geofenced area about ten minutes before the robbery, and headed toward a residential area of town immediately after leaving the bank.

Following further police work, a federal grand jury charged Chatrie with robbery and related firearms offenses. He moved to suppress the information that the police had obtained from Google. According to Chatrie, the officers had acquired that data through a Fourth Amendment search, and the warrant ostensibly authorizing that search was invalid.

The District Court mainly agreed with Chatrie's Fourth Amendment analysis, but still denied the motion to exclude the Location History evidence. Even though “this particular geofence warrant plainly violates the rights enshrined in [the Fourth] Amendment,” the court stated, the officers' reliance

on it was not “objectively unreasonable.” 590 F.Supp.3d at 905, 938. And because that was so, the court concluded, the good-faith exception to the exclusionary rule permitted admission of the location data. See *id.*, at 937–938; *United States v. Leon*, 468 U.S. 897, 922–923, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984) (establishing good-faith exception).

A divided panel of the Court of Appeals of the Fourth Circuit affirmed, but on different reasoning. The majority held that the government did not conduct a search and therefore did not need a warrant. That was so, the majority reasoned, because Chatrie “did not have a reasonable expectation of privacy in two hours’ worth of Location History data voluntarily exposed to Google.” 107 F.4th 319, 325 (2024). Judge Wynn dissented, arguing that “the police intrusion into Chatrie’s Location History data” was “a search that triggered the Fourth Amendment’s protections,” and that the warrant issued was “so lacking in particularity and probable cause that it was invalid.” *Id.*, at 339, 362, and n. 12.

After granting rehearing en banc, the Fourth Circuit affirmed in a one-sentence *per curiam*. See 136 F.4th 100, 101 (2025) (“The judgment of the district court is *AFFIRMED*”). In multiple accompanying writings, the court divided evenly (7 to 7) on whether a Fourth Amendment search had occurred. Of the seven judges who thought it had, most believed the geofence warrant defective. But most also thought the exclusionary rule’s good-faith exception applied, so ruled against Chatrie anyway.

We granted certiorari solely on the question whether the police violated the ***2204** Fourth Amendment in obtaining Chatrie’s location data, thus declining to consider the exclusionary rule issue. See 607 U. S. 1148, — S.Ct. —, 223 L.Ed.2d 553, 2026 WL 120676 (2026). The disputed Fourth Amendment question divides into two parts. First, did law enforcement officials conduct a search under the Fourth Amendment when they acquired Chatrie’s location data from Google? We hold that they did because an individual has a legitimate expectation of privacy in his cell-phone location data. Second, did the multi-step geofence warrant issued here make that search reasonable? We leave that question—which requires deciding whether the warrant satisfied the Fourth Amendment’s probable cause and particularity requirements at each stage of the search process—to the Court of Appeals to address in the first instance.⁴

II

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.” The “basic purpose” of that Amendment, our precedents say, is “to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.” *Carpenter v. United States*, 585 U.S. 296, 303, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018) (quoting *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967)).

That purpose is central to decisions about whether a Fourth Amendment “search” has occurred. Our early search doctrine focused on whether law enforcement officials “obtain[ed] information by physically intruding”—that is, trespassing—on private property. *United States v. Jones*, 565 U.S. 400, 406–407, n. 3, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012); see *id.*, at 404–405, 132 S.Ct. 945. But the Court in *Katz v. United States*, 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), recognized that “the Fourth Amendment protects people, not places.” And so we have long held that “property rights are not the sole measure” of a constitutional violation; the Fourth Amendment “protect[s] certain ***2205** expectations of privacy as well.” *Soldal v. Cook County*, 506 U.S. 56, 64, 113 S.Ct. 538, 121 L.Ed.2d 450 (1992); *Carpenter*, 585 U.S., at 304, 138 S.Ct. 2206. “When an individual seeks to preserve something as private and his expectation of privacy is one that society is prepared to recognize as reasonable,” then governmental “intrusion into that private sphere generally qualifies as a search.” *Ibid.*⁵

Whether an expectation of privacy counts as legitimate is less the result of any fixed set of rules than of “guideposts” stretching back to the Fourth Amendment’s beginnings. *Id.*, at 305, 138 S.Ct. 2206. From the founding onward, we have explained, the Fourth Amendment has sought to secure the “privacies of life” against the exercise of “arbitrary power.” *Boyd v. United States*, 116 U.S. 616, 630, 6 S.Ct. 524, 29 L.Ed. 746 (1886); see *Carpenter*, 585 U.S., at 305, 138 S.Ct. 2206. So too we have recognized, and repeatedly, that the Amendment was designed “to place obstacles in the way of a too permeating police surveillance.” *United States v. Di Re*, 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948); *Carpenter*, 585 U.S., at 305, 138 S.Ct. 2206. Whatever the form of an attempted incursion, the Fourth Amendment protects Americans’ long-held conviction that no government

official should have free access to the most closely kept aspects of their lives.

In recent decades, this Court has often confronted the challenge of adhering to those principles in the face of new technologies. “[I]nnovations in surveillance tools” have “enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes.” *Ibid.* The Court, in response, has sought to “assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). So in one decision, we rejected a “mechanical interpretation” of the Fourth Amendment to hold that the use of a thermal imager to detect heat coming from a person’s home was a search *2206 in the constitutional sense. *Id.*, at 35, 121 S.Ct. 2038. And in another, we held that the search of a cell phone incident to arrest could not proceed without a warrant (even though the search of a handbag could) because of the phone’s “vast quantities of personal information.” *Riley*, 573 U.S., at 386, 134 S.Ct. 2473. Most recently, in *Carpenter v. United States*, this Court held that accessing a form of cell-phone location information other than Location History is a Fourth Amendment search given individuals’ reasonable expectations of privacy. See 585 U.S., at 310–313, 138 S.Ct. 2206.

We begin with *Carpenter* in considering the Government’s front-line position here: that no warrant was needed to get Location History data from Google (although the police “prophylactically secured” one) because no Fourth Amendment search ever took place. See Brief for United States 14. We then explain why the result we reached in *Carpenter* once again follows. Contrary to the Government’s view, an individual has a legitimate expectation of privacy in the information Location History collects about his cell phone’s—meaning his own—movements. The police invade that expectation, and thus conduct a search, when they acquire that information, even though for only a limited period of time and even though via a third-party tech company.

A

The question presented in *Carpenter* was “whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user’s past movements.” 585 U.S., at 300, 138 S.Ct. 2206. The cell-phone records at issue

were what is known as cell-site location information (CSLI). As we explained, CSLI is a “time-stamped record” generated each time a cell phone connects to a cell site. *Id.*, at 301, 138 S.Ct. 2206. Wireless carriers collect and store that information for their own business purposes (such as finding weak spots in their networks). But CSLI can also benefit law enforcement, because it identifies an individual’s approximate location every time his phone makes a connection. In *Carpenter*, police officers investigating a string of Radio Shack robberies ordered a wireless carrier of a known suspect to turn over his CSLI records for a seven-day period (without first getting a warrant). Those records showed, as the Government later put it, that the suspect, Timothy Carpenter, was “right where the ... robbery was at the exact time of the robbery.” *Id.*, at 303, 138 S.Ct. 2206. Carpenter moved to exclude the CSLI records, arguing that the Government acquired them through an unconstitutional search.

The Court began its analysis by reviewing what it had said about a different way of tracking “physical location and movements”: the use of a GPS device to monitor a vehicle. *Id.*, at 306, 138 S.Ct. 2206. In *United States v. Jones*, 565 U.S. 400, 132 S.Ct. 945, 181 L.Ed.2d 911, five Justices had agreed that such tracking counts as a Fourth Amendment search because “individuals have a reasonable expectation of privacy in the whole of their physical movements.” *Carpenter*, 585 U.S., at 310, 138 S.Ct. 2206; see *Jones*, 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring in judgment); *id.*, at 415, 132 S.Ct. 945 (SOTOMAYOR, J., concurring).⁶ That made sense, the *Carpenter* Court thought, even though the movements occurred in public. Prior to the digital age, pursuing a suspect “for any extended period of time was difficult *2207 and costly and therefore rarely undertaken.” 585 U.S., at 310, 138 S.Ct. 2206 (quoting *Jones*, 565 U.S., at 429, 132 S.Ct. 945 (opinion of ALITO, J.)). As a result, “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.” *Carpenter*, 585 U.S., at 310, 138 S.Ct. 2206 (quoting *Jones*, 565 U.S., at 430, 132 S.Ct. 945 (opinion of ALITO, J.)). A new technology should not transform what individuals had reasonably thought they could withhold from the Government.

It followed *a fortiori*, *Carpenter* held, that “[a]llowing government access to cell-site records contravenes” expectations of privacy. 585 U.S., at 311, 138 S.Ct. 2206. To an even greater degree than GPS monitoring, CSLI can provide a full “record of the holder’s whereabouts”

and, with that, “an intimate window into a person's life.” *Ibid.* People, after all, “regularly leave their vehicles,” but they “compulsively carry” their cell phones “all the time.” *Ibid.* A cell phone thus “tracks nearly exactly the movements of its owner”: It “faithfully follows” him not only through “public thoroughfares [but] into private residences, doctor's offices, political headquarters, and other potentially revealing locales.” *Ibid.* What is more, the “newfound tracking capacity” that CSLI gives the police “runs against everyone”—not just those “under investigation”—and “travel[s] back in time.” *Id.*, at 312, 138 S.Ct. 2206. Police officers need not decide in advance (as they do with GPS devices) who they want to follow and when. Instead, they can easily and cheaply—with “just the click of a button”—reconstruct any person's movements “retrospective[ly].” *Id.*, at 311–312, 138 S.Ct. 2206. What in the past was “unknowable” suddenly becomes open to view, presenting formerly unimaginable “privacy concerns.” *Ibid.* The Court thus concluded: “[W]hen the Government accessed CSLI from the wireless carriers”—thereby obtaining a “detailed log” of where Carpenter had gone for seven days—“it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.” *Id.*, at 312–313, 138 S.Ct. 2206.⁷

B

The resemblances between CSLI and Location History, in their relationship to *2208 personal privacy, practically leap off the page. Everything *Carpenter* relied on to find that law enforcement officers conducted a Fourth Amendment search when they accessed wireless carriers' CSLI records applies as well or better to the police's accessing of Google's Location History data.

First, Location History provides an even more fine-tuned picture of a person's movements than CSLI. *Carpenter* noted that through CSLI records, police could “achieve[] near perfect surveillance” of an individual holding a cell phone. *Id.*, at 311–312, 138 S.Ct. 2206. But Location History is nearer perfect still. Here is one way of comparing the two: At any given time, CSLI placed Carpenter within a “sector ranging from one-eighth to four square miles,” whereas Location History pinpointed Chatrrie's location within around twenty meters, which is less than two percent of a mile. *Id.*, at 312, 138 S.Ct. 2206; see 1 App. 45, 3 *id.*, at 173–174. Or here is another measure: CSLI logged Carpenter's location an average of 101 times a day, whereas Location

History commonly records a person's location every two minutes, for a daily average of 720 chartings. See *Carpenter*, 585 U.S., at 302, 138 S.Ct. 2206; 136 F.4th at 151 (Berner, J., concurring). Or finally, a third: Unlike CSLI, Location History can estimate a phone's elevation—so, for example, can tell whether someone has gone into a doctor's office on the first floor of a multi-story building, or a private apartment on the tenth. Of course, the accuracy of each of the two techniques may vary in different places and at different times. But across the board Location History is the far more precise measure. When the *Carpenter* Court said that CSLI provides a “detailed” and “encyclopedic” portrait of a person's whereabouts, it did not know what further technology was on the horizon. 585 U.S., at 309, 138 S.Ct. 2206.

And next, Location History also allows police officers to reconstruct “retrospective[ly],” and with no real effort, people's comings and goings in any area. *Id.*, at 312, 138 S.Ct. 2206. As with CSLI, the Government need not decide in advance the kind of surveillance it should undertake, whether of a person or a site. “Whoever the suspect turns out to be,” *Carpenter* said of CSLI, “he has effectively been tailed every moment of every day.” *Ibid.* Likewise, as this case shows, wherever a location of interest turns out to be (whether a crime scene or a protest march or even a private home), it has effectively been surveilled for the same boundless time. Google's Location History will be available to chart the movements of many individuals—or a few or one—within the vicinity, again at the “click of a button.” *Id.*, at 311, 138 S.Ct. 2206. Recall that in *Jones*, it was thought notable that law enforcement officials of an earlier age usually could not monitor every movement of an individual's car, as a GPS device does. See *supra*, at 2206 - 2207; 565 U.S., at 430, 132 S.Ct. 945 (opinion of ALITO, J.); see also *Carpenter*, 585 U.S., at 312, 138 S.Ct. 2206 (“In the past, attempts to reconstruct a person's [prior] movements were limited”). Far less could those officials ever perform the “tireless and absolute surveillance” of any number of people in any number of places, public and private, that Location History can accomplish. *Ibid.* If the one kind of intrusion clashes with “society's expectation[s]” of what counts as private, so must the other. *Jones*, 565 U.S., at 430, 132 S.Ct. 945 (opinion of ALITO, J.).

Indeed, Location History records implicate those privacy interests still more than CSLI data because the former is more the individual's own. Most cell-phone users have no awareness of CSLI records, and anyway would never try to retrieve them. *2209 The records are instead the province

of wireless carriers, which maintain them for an array of business functions. See *Carpenter*, 585 U.S., at 301, 138 S.Ct. 2206; *supra*, at 2205 - 2207. Location History information is different. No doubt, Google itself uses those records to improve the quality of its apps. But Google users, too, regularly employ Location History—for example, “to remind themselves of a restaurant they ate at two weeks ago, the time they were last at a friend’s home, the sites they saw on vacation, or the distance they walked on a particular day.” Brief for Google LLC as *Amicus Curiae* 8. The records thus serve as a personal journal of a user’s movements, which that user consults (and even can edit) for his own purposes. See *id.*, at 10. In that way, Location History resembles other private materials—think of emails, documents, photographs, or calendars—that even if stored on Google’s servers, a user reasonably views as his own. And as a result, that he reasonably expects to be shielded from the “inquisitive eyes” of the government. *Carpenter*, 585 U.S., at 305, 138 S.Ct. 2206.

C

The Government, not much contesting any of the above, principally argues on a different ground: that accessing only a short amount of cell-phone location information (whether Location History or CSLI) does not count as a Fourth Amendment search. (The dissent likewise contends that the “duration” of data obtained here is too brief for a search to have happened. *Post*, at 2230 (ALITO, J.); see *post*, at 2230 - 2231.) Recall that *Carpenter* involved seven days’ worth of location data. See *supra*, at 2206 - 2207. And in deciding that case, this Court reserved the issue whether there was a more “limited period for which the Government may obtain” such data “free from Fourth Amendment scrutiny.” 585 U.S., at 310, n. 3, 138 S.Ct. 2206.⁸ The Government now claims that the answer is yes, and that the two hours’ worth of Location History acquired here falls within the Constitution-free zone. In the Government’s view, a person has no reasonable expectation of privacy in “that short a time window” of location data, because his “short-term” movements will “reveal[] little about the details of [his] personal life.” Brief for United States 12, 20; see *id.*, at 20 (“A single stop at a doctor’s office, for example, does not in itself identify the reason for the visit”). The Government cites in support *United States v. Knotts*, 460 U.S. 276, 282, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), in which the Court held that police officers’ use of a beeper to assist an hours-long tail of a car did not bring the Fourth Amendment into play.

The lesson the Government draws is that law enforcement officials accessing Location History should receive a Fourth Amendment grace period of some number of hours.

But to begin, the Government is wrong about the incapacity of short-term location *2210 information to reveal private matters. “[R]epeated patterns,” in the Government’s phrasing, are not all that individuals wish to, and reasonably expect to, keep to themselves. Brief for United States 20. Return here to another of *Jones*’s insights: “[E]ven short-term monitoring” of a person’s physical movements can provide “a wealth of detail about [his] familial, political, professional, religious, and sexual associations.” 565 U.S., at 415, 132 S.Ct. 945 (opinion of SOTOMAYOR, J.). Consider just a few trips that a person is apt to think “indisputably private”: to “the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, [or] the by-the-hour motel.” *Ibid.* And unlike a GPS device, Location History enables police officers to focus on precisely those sites—to see, in a given time block, who shows up. Similarly, Location History—even two hours of it—allows officers to target one-off events of potential interest: a gun show, say, or a political rally.

Still more fundamentally, we have never understood Fourth Amendment protections as kicking in only once an intrusion “goes too far.” *Pennsylvania Coal Co. v. Mahon*, 260 U.S. 393, 415, 43 S.Ct. 158, 67 L.Ed. 322 (1922) (adopting that approach for regulatory takings). Where the Fourth Amendment applies, it applies—regardless of “the quality or quantity of information” the government obtains. *Kyllo*, 533 U.S., at 37, 121 S.Ct. 2038. So, for example, this Court held that thermal imaging qualified as a search even though it did not, and was not likely to, detect “private activities” or “intimate details.” *Ibid.* The Amendment, we analogized, makes “no exception” for the officer “who barely cracks open the front door and sees nothing but the nonintimate rug on the vestibule floor.” *Ibid.* And likewise, the Amendment does not give agents a pass if their wiretap is of limited duration and thus less likely to intrude on private matters. Indeed, in our seminal wiretap case, the police obtained only 18 minutes of recordings. See *Katz*, 389 U.S., at 354, n. 14, 88 S.Ct. 507.

That approach makes all the more sense when, as with Location History, officials can select the time-limited set of materials they want from an all-encompassing database. Then, the durational bounds on the data actually acquired do little to address the Fourth Amendment’s concern about “a too permeating police surveillance.” *Di Re*, 332 U.S.,

at 595, 68 S.Ct. 222; see *supra*, at 2205. What creates that concern is that the government can access all of a cell-phone user's movements, in both public and private places—that it possesses a virtual panopticon with which to scrutinize its citizens' activities. The sweep of the official invasion is not made less because the government, with the benefit of hindsight, can pinpoint exactly which few hours of movements it wants to review. That feature of accessing location data is, indeed, more a practical benefit to the government than a limit on its intrusive powers.⁹

And contra the Government, *Knotts* does not support the view that accessing *2211 two hours of Location History is not a search. There, police officers put a beeper in a car to help them follow it from Minnesota to Wisconsin. The Court decided that the beeper did not turn the tail into a search, but was explicit in keeping its holding cabined to that rudimentary technology. The defendant had argued that a ruling against him would enable officials to conduct “surveillance of any citizen of this country” free from the strictures of the Fourth Amendment. 460 U.S., at 283, 103 S.Ct. 1081. The Court took the concern seriously, stating that if technology progressed so as to allow more sophisticated surveillance, “different constitutional principles” could well apply. *Id.*, at 284, 103 S.Ct. 1081. And three decades later, five Justices in two opinions found that they did. When faced in *Jones* with a GPS device—which unlike the beeper allowed remote monitoring—they decided, notwithstanding *Knotts*, that privacy was implicated and a search had occurred. See *supra*, at 2206 - 2207. Yet even that was not all. When six years further on, the *Carpenter* Court held that accessing CSLI was a search, it recounted the *Knotts*-to-*Jones* progression to explain why *Knotts* did not stand in its way. See 585 U.S., at 306–307, 138 S.Ct. 2206 (*Knotts* “was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance”). For the third time, we reach the same conclusion today.

And still another feature of *Knotts* makes it inapt here: that the surveillance there was confined to public roads. That fact was crucial to the Court's decision: “A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy,” *Knotts* explained, because the car is always “in plain view.” 460 U.S., at 281, 103 S.Ct. 1081. By contrast, the movements that Location History reveals are not limited to public streets. Recall what *Carpenter* observed: A “cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, [and] political headquarters.” 585 U.S., at 311, 138 S.Ct.

2206; see *supra*, at 2207.¹⁰ In one of those places—a private residence—this Court has held even beeper technology to count as a search because it could reveal “whether a particular article—or a person, for that matter” was in the home “at a particular time.” *United States v. Karo*, 468 U.S. 705, 716, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984). If that is so, accessing Location History must also be a search—even if for only two hours—because that data can far more reliably show someone within a home (indeed, on a specific floor). The Government replies with an odd argument. It thinks *2212 that “tracking [someone] into a private residence”—yes, even for two hours—would “probably” be a search, but tells us not to worry because Chatrrie did not go home. Tr. of Oral Arg. 98, 134. That approach, however, is foreign to the way the Fourth Amendment works. Whether something is a search does not depend on what it finds. See *Di Re*, 332 U.S., at 595, 68 S.Ct. 222 (“[A] search is not to be made legal by what it turns up. In law it is good or bad when it starts”). An officer, after all, cannot know the fruits of a given surveillance in advance. The surveillance must be either a search or not regardless. The Government's concession thus gives away its argument that, for purposes of the Fourth Amendment, two hours of cell-phone location data is not enough.

D

The Government has an additional argument, which in *Carpenter* was its “primary” one—that the so-called third-party doctrine precludes Chatrrie from invoking the Fourth Amendment's protections. 585 U.S., at 313, 138 S.Ct. 2206. (Here too the dissent reiterates the Government's view. See *post*, at 2228 - 2229, 2231 - 2232 (ALITO, J.).) The idea is that in “authoriz[ing] Google to collect, retain, and use” his location information, Chatrrie lost his legitimate expectation of privacy, and therefore his right to complain of a search—regardless whether it was for two hours, two weeks, or two years. Brief for United States 15. The problem for the Government—and presumably the reason that its primary assertion in *Carpenter* has here become a secondary one—is that *Carpenter* refused to apply the third-party doctrine to CSLI, and no good reason exists to reach a different result for Location History.

The third-party doctrine traces to two cases involving information provided by customers to a bank and telephone company, and then turned over to law enforcement officials. In *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), this Court held that a bank depositor had

no reasonable expectation of privacy in canceled checks and deposit slips in his bank's possession, because the records were “voluntarily conveyed to the bank[] and exposed to [its] employees in the ordinary course of business.” *Id.*, at 442, 96 S.Ct. 1619. The depositor, the Court explained, had “take[n] the risk, in revealing his affairs to another,” that the third party would in turn provide that information to the government. *Id.*, at 443, 96 S.Ct. 1619. A few years later, the Court in *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), applied that principle to hold that a (landline) telephone subscriber lacked a legitimate expectation of privacy in the phone numbers he dialed. Once again, the Court reasoned that the subscriber had “voluntarily conveyed [the dialed numbers] to the telephone company,” and so relinquished his Fourth Amendment right. *Id.*, at 744, 99 S.Ct. 2577.

In *Carpenter*, however, the Court rejected the Government's contention that the third-party doctrine likewise governed the acquisition of CSLI. The Court acknowledged that a cell-phone user “continuously reveals his location” to a third-party wireless carrier. 585 U.S., at 309, 138 S.Ct. 2206. But it held that cell-phone location information is “qualitatively different” from “telephone numbers and bank records.” *Ibid.* Those differences fell along two axes. First, the Court explained, the “nature” of CSLI is incomparably “revealing.” *Id.*, at 314, 138 S.Ct. 2206. There is “a world of difference” between the “exhaustive chronicle of location information casually collected by wireless carriers” and “the limited types of personal information addressed in *Smith* and *Miller*.” *Ibid.* The former thus “implicates privacy concerns *2213 far beyond” the latter. *Id.*, at 315, 138 S.Ct. 2206. And second, the Court continued, “[c]ell phone location information is not truly ‘shared’ as one normally understands the term.” *Ibid.* Because “cell phones and the services they provide” are “such a pervasive and insistent part of daily life”—“indispensable to participation in modern society”—a person can hardly help but generate a “trail of location data.” *Ibid.* “[I]n no meaningful sense,” the Court thought, does that mean a person “voluntar[il]y expos[es]” to any third party a “comprehensive dossier of his physical movements.” *Ibid.*

Both differentiating features highlighted in *Carpenter* apply equally or better to Location History. As noted above, Location History is even more “revealing” than CSLI, because it provides a yet more precise record of an individual's movements. See *supra*, at 2207 - 2208. Access to that record enables officials to undertake nearly perfect, retrospective surveillance of countless persons and places.

See *supra*, at 2208 - 2209. And for Location History, that surveillance is based on information that a user reasonably understands as his own, even though stored on Google's servers—much like his emails, photos, and calendar entries. See *supra*, at 2208 - 2209. Likewise, the information is “not truly shared,” in the normal sense of wanting a third party to see or use it. *Carpenter*, 585 U.S., at 315, 138 S.Ct. 2206. The exposure of that information to Google is merely what happens when a user avails himself of one of the services on his cell phone. Or said a bit differently, it is the automatic price of conventional cell-phone usage—which, just as *Carpenter* noted, is a “pervasive and insistent part of daily life.” *Ibid.* So just as the third-party doctrine did not apply in *Carpenter*, it does not apply here.

The Government contests that conclusion on *Carpenter*'s second axis alone: It claims that generating Location History, unlike producing CSLI, is a voluntary choice on the user's part. Although carrying a cell phone may be indispensable in modern society, the Government argues, using Location History is not. Rather, Location History is an “optional add-on,” which a user must enable by an “affirmative act” beyond “powering up” a phone. Brief for United States 13, 22 (quoting *Carpenter*, 585 U.S., at 315, 138 S.Ct. 2206). In support, the Government emphasizes that only around one-third of current Google accountholders have activated the service. See Brief for United States 22; see 1 App. 45. That goes to show, says the Government, that people can “live[] without” Location History. Brief for United States 22; see Tr. of Oral Arg. 92. And if that is true (the Government says), people who do use the feature have indeed “voluntar[il]ly expos[ed]” all of their movements. *Carpenter*, 585 U.S., at 315, 138 S.Ct. 2206.

But as an initial matter, that argument ignores some pertinent facts about how and why Google users turn on Location History. As described earlier, Google prompts a user, and repeatedly, to turn on the service—when he sets up a Google account, when he sets up an Android phone, and when he sets up a Google app. See *supra*, at 2200 - 2201. The prompt often informs him that his device will not “work correctly” unless he does so. 2 App. 140–141. By contrast, it does not tell him quite what he is signing up for: “how frequently Google would record [his] location”; “how precise Location History can be”; or how Google might give all that minute-by-minute location information to the government. 590 F.Supp.3d at 936; 136 F.4th at 128 (Wynn, J., concurring in judgment). In those circumstances, it is hard to see how any user is, in the normal sense, “sharing” with third parties a comprehensive

catalog of his physical movements. *Carpenter*, 585 U.S., at 314, 138 S.Ct. 2206. *2214 And that is so regardless of how many others ignore Google's entreaties. The Government's estimation of that number is almost surely overstated: It appears to include, for example, the many millions of Google accountholders in foreign countries like China where collecting Location History is illegal. See 4 Joint App. in No. 22-4489 (CA4), pp. 845, 848. But in any event, the raw user totals for Location History—one-third, two-thirds, or someplace in between—are not the most apt measure of whether that service's enlistees have, as the Government claims, self-consciously “assumed the risk of sharing” all their movements with others. Brief for United States 12.

More generally, the Government's approach to Fourth Amendment protection would raise a host of workability issues. At the top of the list: What percentage of users would have to sign up for a service to make doing so non-voluntary? The Government posited at argument that if 80 percent of active Google accountholders had enabled Location History, the case would be “much closer.” Tr. of Oral. Arg. 92. After all, the Government candidly noted, even possessing a cell phone is not truly “indispensable” (to use *Carpenter*'s word): “[S]omething like 90 percent of people have [them].” Tr. of Oral. Arg. 92. So where to draw the line? And after that, the questions only multiply. Would a user lose Fourth Amendment protection if a highly popular cell-phone feature became less so over time? What if the use of a given feature is ubiquitous among (but only among) a subset of the population (say, an age cohort), and an individual defendant is a member of that class? Would it be enough if the lion's share of cell-phone users enabled a feature similar to the one at issue—so, for example, any location-tracking service, whether Google's or some other company's? And finally, a more basic inquiry: In such a world, how is anyone—whether a cell-phone user or a police officer—to know in advance (which is when the knowledge is useful) whether enrollees in a given service will be found to have Fourth Amendment protection in the information that service collects? To ask all these questions about the Government's approach is to know that it is on the wrong track.

And there is yet a deeper problem: The Government's app-by-app, feature-by-feature method of granting Fourth Amendment protection misapprehends the very nature of modern cell-phone use. Pretty much everything a person does on a smartphone requires some kind of opt-in—an “affirmative act” beyond “powering up” to utilize a given app or service. *Carpenter*, 585 U.S., at 315, 138 S.Ct.

2206. Consider sending an email on Gmail, uploading a photo to Google Photos, or adding a calendar entry to Google Calendar. None happens solely by dint of the phone's operation; each requires, as Location History does, an “optional add-on.” Brief for United States 13. And each activity, like using Location History, results in sharing information with a third-party tech company—turning over private materials to live on that company's servers. The Government wishes to disconnect all those uses from the mere act of carrying a turned-on cell phone (the thing that generates CSLI), with only the latter receiving assured Fourth Amendment protection. But that is to imagine that all of us are living in dumb flip-phone days. The point of carrying smartphones is to use what is on them—as *Carpenter* said, to use the apps and “services they provide.” 585 U.S., at 315, 138 S.Ct. 2206. *That* is what has become a “pervasive and insistent”—even “indispensable”—“part of daily life.” *Ibid.*; *Riley*, 573 U.S., at 385, 134 S.Ct. 2473. And so *that* is what *Carpenter* insulated from the third-party doctrine. A cell-phone user *2215 is not to be viewed as sharing private information with third parties—which then can be freely passed on to the government—just by doing the ordinary things cell-phone users do.

* * *

For all those reasons, we hold that police officers invade a cell-phone user's reasonable expectation of privacy when they access his Location History. It does not matter if the time period scrutinized was only two hours. Nor does it matter that the materials obtained were handed over by a third-party tech company. When the government “accesses historical cell phone” location information—Location History as much as CSLI—it “conducts a search under the Fourth Amendment.” *Carpenter*, 585 U.S., at 300, 138 S.Ct. 2206.

III

That conclusion does not resolve this case, because the Fourth Amendment prohibits only searches that are “unreasonable.” When law enforcement officials undertake a search to discover evidence of a crime, the reasonableness standard generally requires that they seek a warrant from “a neutral and detached magistrate.” *Johnson v. United States*, 333 U.S. 10, 14, 68 S.Ct. 367, 92 L.Ed. 436 (1948); see *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995).¹¹ That requirement subjects the officials' assessment of a search's propriety to the “deliberate,

impartial judgment of a judicial officer.” *United States v. Grubbs*, 547 U.S. 90, 99, 126 S.Ct. 1494, 164 L.Ed.2d 195 (2006). The magistrate, in turn, may issue a warrant only when “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).

When officers have obtained a warrant, as they did here, a search's legality will thus depend on whether a magistrate has properly found probable cause to support a particularly described search. “[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” *Illinois v. Gates*, 462 U.S. 213, 232, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). But a magistrate must always determine that there is a “fair probability that contraband or evidence of a crime will be found” in the place searched. *Id.*, at 238, 103 S.Ct. 2317. That means determining, to the requisite “fair probability,” both that the place searched will have the materials sought and that those materials will contain evidence “aid[ing]” in a criminal’s “apprehension or conviction.” *Messerschmidt v. Millender*, 565 U.S. 535, 551, 552, n. 7, 132 S.Ct. 1235, 182 L.Ed.2d 47 (2012); see *Zurcher v. Stanford Daily*, 436 U.S. 547, 556, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978) (“The critical element” is whether there is the requisite “cause to believe that the specific ‘things’ to be searched for and seized are located” in the targeted place). The particularity requirement, for its part, ensures that the search will be of an appropriate scope—that it is “carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.” *2216 *Maryland v. Garrison*, 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987). That requirement typically looks to such matters as the geographic and durational expanse of the search. See *id.*, at 84–85, 107 S.Ct. 1013; *Karo*, 468 U.S., at 718, 104 S.Ct. 3296. And it too must take account of “particular factual contexts,” including in surveillance cases the nature of the technology to be used. *Gates*, 462 U.S., at 232, 103 S.Ct. 2317; see, e.g., *Karo*, 468 U.S., at 718, 104 S.Ct. 3296; see generally Kerr Brief 17–20.

The warrant issued here, as described earlier, was an uncommon, multi-step one. See *supra*, at 2202 - 2203. The first step it laid out authorized police officers to obtain location data for all cell phones inside the designated geofence within a one-hour timeframe. The second step entitled the officers to obtain additional data (two hours, both inside and outside the geofence) for a subset of those phones—of the

officers’ own choosing. And the third step enabled them to obtain personal identifying information (including names, email addresses, and phone numbers) for a further subset—again of their selection. As to how the officers would make their choices at the second and third steps—how they would pick the users subject to more intense scrutiny—the warrant said very little. *In toto*: They would “attempt to narrow down the list by reviewing the time stamped location coordinates for each [device] and comparing that against the known time and location information that is specific to this crime.” 2 App. 136; see *id.*, at 137; *supra*, at 2202 - 2203.

The parties have contested the legality of each stage of that process. Chatrie analogizes the first step to an “unconstitutional general warrant,” and argues that in any event the search at that step was both insufficiently described by the warrant and lacking in probable cause. Brief for Chatrie 12; see *id.*, at 13. As to steps two and three, Chatrie contends that the warrant left too much authority to police officers—and too little to the magistrate—to define the search's scope and determine whether cause for it existed. See *id.*, at 13–14. The Government, for its part, defends the warrant at every step as seeking “particularized information from Google's database” based on “probable cause to believe that Google had information” that would help solve a crime. Brief for United States 14. And the Government urges that the discretion given to the officers at steps two and three fell within the bounds of reasonableness. See *id.*, at 46.

We leave all of those questions to the Court of Appeals to decide in the first instance. Because the Fourth Circuit panel concluded that no search had occurred, it did not address whether the geofence warrant issued here validly authorized each stage of the search process. Nor did the en banc court's one-sentence *per curiam* opinion speak to that issue. We are, as we have said many times before, “a court of review, not of first view.” *Cutter v. Wilkinson*, 544 U.S. 709, 718, n. 7, 125 S.Ct. 2113, 161 L.Ed.2d 1020 (2005). It is therefore now up to the Court of Appeals to decide whether, at each step of the search process, the warrant satisfied the Fourth Amendment's requirements of particularity and probable cause.

IV

In his famed and vindicated dissent, Justice Brandeis explained why a wiretap was a search, subject to Fourth Amendment requirements. See *Olmstead v. United States*, 277 U.S. 438, 471, 48 S.Ct. 564, 72 L.Ed. 944 (1928). Those

who drafted the Amendment could not have imagined such a technology. But they understood, Justice Brandeis wrote, a matter of more transcendent importance: that Americans had “as against the Government, the right to *2217 be let alone” and that the Fourth Amendment must protect against “every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed.” *Id.*, at 478, 48 S.Ct. 564.

Far more recently, this Court in *Carpenter* invoked Justice Brandeis's opinion in explaining why law enforcement officials could not have “unrestricted access to a wireless carrier's database of physical location information.” 585 U.S., at 320, 138 S.Ct. 2206. Said *Carpenter*: “[T]he Court is obligated—as [s]ubtler and more far-reaching means of invading privacy have become available to the Government—to ensure that the ‘progress of science’ does not erode Fourth Amendment protections.” *Ibid.* (quoting 277 U.S., at 473–474, 48 S.Ct. 564 (dissenting opinion)). For new technological tools, the Court continued, may “risk[] Government encroachment of the sort the Framers, after consulting the lessons of history, drafted the Fourth Amendment to prevent.” 585 U.S., at 320, 138 S.Ct. 2206.

Today's decision follows from the same judicial obligation, to guard against the same risk of undue encroachment. The Fourth Amendment applies, too, when officials tap into Google's “database of physical location information.” *Ibid.* That database is new, but the principle covering it is not: That principle is instead the one our history has given. The Fourth Amendment must, as ever, protect against unjustified governmental intrusion on the privacy of the individual.

For the reasons stated, we vacate the judgment of the Court of Appeals and remand the case for further proceedings consistent with this opinion.

It is so ordered.

Justice JACKSON, with whom Justice SOTOMAYOR joins, concurring.

I agree with the Court that law enforcement officers conducted a search when they accessed petitioner Chatric's Location History. I write separately because I would have gone further to explain that this search violated the Fourth Amendment. As the Court observes, “[w]hen officers have obtained a warrant,” the validity of a search turns on “whether a magistrate has properly found probable cause to support a particularly described search.” *Ante*, at 2215. In my view,

it is clear that at a minimum the second and third stages of the search process here did not satisfy this foundational requirement.

At step two, the warrant authorized officers to access an additional hour's worth of Location History, unbounded by the geofence's perimeter. Though the warrant stated that officers would “attempt to narrow down the list” of devices subject to this step, there was no explicit requirement that they do so. 2 App. 136 (emphasis added). Nor did the warrant set forth any criteria that officers would use in their narrowing efforts. *Ibid.*

The same infirmities carried over to step three. At this step, the warrant authorized officers to access “identifying account information,” including the username, date of birth, account number, and any email addresses or telephone numbers associated with the account. *Id.*, at 137. Once again, the warrant stated only that officers would “attempt to narrow down the list,” without setting forth any criteria for doing so. *Ibid.* (emphasis added).

This “uncommon, multi-step” process, *ante*, at 2215 – 2216, meant that officers conducted key portions of the search outside the supervision of “a neutral and detached magistrate,” *Johnson v. United States*, 333 U.S. 10, 14, 68 S.Ct. 367, 92 L.Ed. 436 (1948). Put differently, officers could obtain additional, sensitive information at steps two and three without having *2218 to convince a magistrate that there was probable cause to believe this particular information would uncover evidence related to the crime. In this way, the warrant left “too much to the discretion of the officer[s] executing the order,” giving them a “roving commission” to collect more data absent any justification to a magistrate. *Berger v. New York*, 388 U.S. 41, 59, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967).

The facts of this case illustrate why the lack of magisterial oversight is dangerous. When executing steps two and three, law enforcement initially sought unbounded data and account information from *all* 19 devices identified at step one. See 590 F.Supp.3d 901, 921 (ED Va. 2022). Nothing in the warrant prevented officers from obtaining this broad set of data; they narrowed the list only because Google insisted on it. The officers eventually settled on requesting data from nine devices at step two, but even this shorter list may have been overbroad. For three of the nine devices, the location data showed the users' movements to and from sensitive spaces—namely, residences, a school, and a hospital. See *id.*, at 923. Given how it was written, the warrant itself provided

no “judicial check” on law enforcement’s determination that probable cause justified this intrusion. *Steagald v. United States*, 451 U.S. 204, 220, 101 S.Ct. 1642, 68 L.Ed.2d 38 (1981).

* * *

The Court correctly observes that allowing the Government to “access all of a cell-phone user’s movements” without limit essentially arms it with “a virtual panopticon with which to scrutinize its citizens’ activities.” *Ante*, at 2210. It is for this reason that law enforcement and courts must carefully abide by the Fourth Amendment’s instruction 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.” The Fourth Circuit should keep this instruction in mind on remand when evaluating the constitutionality of the multi-step search that occurred here, especially at steps two and three.

Justice GORSUCH, concurring in the judgment.

I agree with the Court’s judgment that the government’s examination of Okello Chatrie’s Location History data amounted to a search for purposes of the Fourth Amendment. But respectfully, I would reach that conclusion by a different route.

I

To decide whether a Fourth Amendment search took place in this case, the Court once again invokes a test first advanced in a solo concurrence in *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). Under that test, a search occurs when the government intrudes on an “expectation of privacy” that “society is prepared to recognize as ‘reasonable.’ ” *Id.*, at 361, 88 S.Ct. 507 (Harlan, J., concurring).

If *Katz* has become a familiar feature of our law, it seems to me no more persuasive for it. Consider just a few of its problems, beginning with this: It has no basis in the Constitution’s text or history. The Fourth Amendment’s protections do not depend on “the breach of some abstract ‘expectation of privacy’ whose contours are left to the judicial imagination.” *Carpenter v. United States*, 585 U.S. 296, 391, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018) (GORSUCH, J., dissenting). Instead, the Fourth Amendment speaks in more concrete terms,

protecting an individual’s person, house, papers, and effects from unreasonable searches and seizures. *Ibid.* No surprise, then, that it’s hard to find anything *2219 like the *Katz* test in the law leading up to the Fourth Amendment’s adoption—or anything much like it in this Court’s jurisprudence before the 1960s. See *Carpenter*, 585 U.S., at 391–392, 138 S.Ct. 2206 (GORSUCH, J., dissenting).

Even if I could overlook that problem with *Katz*, I still wouldn’t know how to apply it. As the Court has candidly admitted, it has never been able to identify a “single rubric” that might “definitively resolv[e] which expectations of privacy are entitled to protection.” *Carpenter*, 585 U.S., at 304, 138 S.Ct. 2206 (majority opinion). Maybe *Katz* poses an empirical question, tagging reasonable expectations of privacy to those privacy expectations “people *actually* have.” *Carpenter*, 585 U.S., at 392, 138 S.Ct. 2206 (GORSUCH, J., dissenting). Or maybe the question is a normative one, asking what expectations reasonable people “*should* ... have.” *Ibid.* In truth, nobody knows and, either way, this Court is the wrong body for the task. We aren’t equipped to make empirical assessments about what most Americans think. Nor is it our job to enforce our own normative judgments, as opposed to those embodied in the Constitution and laws. *Id.*, at 392–394, 138 S.Ct. 2206.

If this weren’t trouble enough, we’ve also adorned *Katz* with an equally indefensible qualification called the third party doctrine. Under its terms, the Court has held, an individual maintains no “reasonable expectation of privacy” in information he shares with others. Accordingly, the government may freely search a person’s papers and effects without triggering any Fourth Amendment scrutiny so long as they are entrusted to the care of someone else. See *Smith v. Maryland*, 442 U.S. 735, 743–744, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); *United States v. Miller*, 425 U.S. 435, 442–443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976).

Much as with *Katz* itself, this Court has never offered a persuasive justification for its offshoot. *Carpenter*, 585 U.S., at 389–390, 138 S.Ct. 2206 (GORSUCH, J., dissenting). Nor do I see how it might. Do we seriously mean to suggest that most Americans think they have no “reasonable expectation of privacy” in records held for them by their banks or pharmacists or doctors or technology companies? If not, on what authority might we rule that the American people should not reasonably expect privacy in materials like those? Really, the third party doctrine amounts to little more than a “doubtful application of *Katz* that lets the government search almost

whatever it wants whenever it wants.” *Id.*, at 391, 138 S.Ct. 2206.

As it did eight years ago in *Carpenter*, the Court today largely ignores these problems. It simply declares that Mr. Chatric enjoyed a reasonable expectation of privacy in his Location History because authorities could have used it to create “a virtual panopticon.” *Ante*, at 2210 - 2211. And it tells us that the third party doctrine does not apply to this case because Mr. Chatric did “ ‘not truly shar[e] ’ ” his Location History with Google. *Ante*, at 2212 - 2213 (quoting *Carpenter*, 585 U.S., at 315, 138 S.Ct. 2206 (majority opinion)).

Count me unpersuaded. Why does tracking Mr. Chatric's movements digitally over an hour or two invade his reasonable expectation of privacy when an officer tailing him for the same length of time would not? See *United States v. Knotts*, 460 U.S. 276, 281–283, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983). Why is Location History data Mr. Chatric voluntarily shared with Google not “truly shared” when a person's bank records are? See *Miller*, 425 U.S., at 440–443, 96 S.Ct. 1619. Does the Court just mean to give *Katz*'s third party doctrine a quiet burial by suggesting today that any information shared over “smartphones” using *2220 “apps and services” falls outside its reach? *Ante*, at 2214 - 2215 (internal quotation marks omitted). And what does any of this have to do with the Fourth Amendment's terms anyway? Even if *Katz* and its battered third party doctrine may straggle on today, they leave our Fourth Amendment jurisprudence about where the Court's obscenity doctrine stood in the 1960s: We know a “reasonable expectation of privacy” (and an exception to the third party doctrine) when we see it.

II

Rather than employ *Katz* and its third party doctrine, I would take a different approach. To decide whether the Fourth Amendment is in play, I would consult its terms, asking first whether Location History qualifies as one of Mr. Chatric's papers or effects, and then asking whether the government searched those papers or effects. This traditional approach remains very much part of our law. See *Byrd v. United States*, 584 U.S. 395, 403, 138 S.Ct. 1518, 200 L.Ed.2d 805 (2018). Indeed, we have expressly recognized that *Katz* and its progeny “supplemen[t] rather than displac[e]” traditional Fourth Amendment principles. *Carpenter*, 585 U.S., at 403, 138 S.Ct. 2206 (majority opinion); see also *Soldal v. Cook County*, 506 U.S. 56, 64–65, 113 S.Ct. 538, 121 L.Ed.2d 450

(1992); *United States v. Jones*, 565 U.S. 400, 406–407, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012); *Florida v. Jardines*, 569 U.S. 1, 11, 133 S.Ct. 1409, 185 L.Ed.2d 495 (2013).

Thanks to *Katz*'s prominence today, of course, litigants sometimes fail to press more traditional Fourth Amendment arguments. See, e.g., *Carpenter*, 585 U.S., at 406, 138 S.Ct. 2206 (GORSUCH, J., dissenting). But whatever his faults (possibly including bank robbery), Mr. Chatric has not forfeited that line of attack in this case. In fact, he begins his brief before us by contending that the Fourth Amendment is implicated here precisely because the government enlisted Google to search his “papers and effects.” See Brief for Petitioner 15, 33.

I agree with that assessment. Set aside whether Location History data qualifies as among Mr. Chatric's “papers,” and consider whether it at least constitutes one of his “effects.” Based on the evidence the parties have put before us, it appears the word “effects” was understood at the time of the Fourth Amendment's adoption to embrace most any kind of personal property. See, e.g., M. Brady, *The Lost “Effects” of the Fourth Amendment: Giving Personal Property Due Protection*, 125 Yale L. J. 946, 985–987 (2016) (“[E]arly sources indicate that the term ‘effects’ meant ‘personal property’ in common and colloquial usage”); L. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1301 (2016) (effects meant “personal property or possessions,” including “commercial items and goods”); Brief for United States 32 (suggesting that “effects” excludes certain real property like so-called open fields (citing *Oliver v. United States*, 466 U.S. 170, 104 S.Ct. 1735, 80 L.Ed.2d 214 (1984))).

As I see it, Mr. Chatric's Location History data qualifies as his personal property. To appreciate why, start with this. As Google puts it, and no one seriously disputes, Location History serves as a “diary” or map “of a person's travels.” Brief for Google LLC as *Amicus Curiae* 3–4. At the time of the events in question, Mr. Chatric's agreement with Google referred to Location History as “your” (meaning, the user's) “information.” 1 App. 72 (emphasis added). Under the parties' agreement, too, Mr. Chatric was free to “review” and “edit” his location data. *Id.*, at 19. He was even free to export or delete that data “from Google's servers at will.” *Ibid.* Beyond all that, Google promised to protect *2221 his information against “unauthorized access, alteration, disclosure, or destruction.” *Id.*, at 71. Put simply, Mr. Chatric had the rights to enjoy, manage, alter, dispose,

and exclude others from what amounted to an electronic diary or map of his travels. And as someone who held that many “sticks in the bundle of rights ... commonly characterized as property”—including the “most treasured” and “essential” right to exclude—he has a strong claim that the Location History data was his personal property. *Cedar Point Nursery v. Hassid*, 594 U.S. 139, 149–150, 141 S.Ct. 2063, 210 L.Ed.2d 369 (2021) (internal quotation marks omitted).

Next, notice what statutory and case law have to say on the subject. The investigation of Mr. Chatrle unfolded in Virginia. That State's Computer Crimes Act expressly describes “computer data” as a form of “[p]roperty.” Va. Code Ann. § 18.2–152.2 (2021). Altering or making an unauthorized copy of computer data can constitute the crime of “computer trespass” (another property law concept). §§ 18.2–152.4(A)(3), (6). And the State provides a right to sue for anyone “whose property or person is injured” by violations of the Act (again suggesting a right to exclude). § 18.2–152.12(A).

Nor is Virginia some outlier. In Texas, “computer ... data” can constitute “[p]roperty.” Tex. Penal Code Ann. § 33.01(16) (West Cum. Supp. 2025). State law likewise criminalizes “knowingly access[ing] ... a computer, computer network, or computer system ... with the intent to obtain or use a file, data, or proprietary information” for a prohibited purpose. § 33.02(b–1)(2)(C) (West 2016). Once more, as well, those whose “property has been injured” by certain computer crimes may bring a “civil cause of action.” Tex. Civ. Prac. & Rem. Code Ann. § 143.001 (West 2019). Georgia has a similar regime. See Ga. Code Ann. §§ 16–9–93(b), (g) (2018) (criminalizing “[c]omputer [t]respas” and providing a private right of action for such violations). And, it appears, so do many other States. See Brief for Cato Institute as *Amicus Curiae* 14–15, and n. 5 (“Today, more than half of states ... treat digital records and data as personal property,” and “[m]any” of them “make it illegal for private actors to access or convert another person's digital data”); see also, e.g., *People v. Seymour*, 536 P.3d 1260, 1273 (Colo. 2023) (finding that “law enforcement's copying of [the defendant's] search history meaningfully interfered with his possessory interest in that data”); *Integrated Direct Marketing, LLC v. May*, 2016 Ark. 281, p. 6, 495 S.W.3d 73, 76 (“[U]nder Arkansas law, intangible property, such as electronic data, ... can be converted”); cf. *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 292–293, 864 N.E.2d 1272, 1278, 832 N.Y.S.2d 873 (2007) (holding that “electronic records that

were stored on a computer and were indistinguishable from printed documents” are “subject to a claim of conversion”).

To be sure, pursuant to its agreement with Mr. Chatrle, Google stored his Location History data on its servers and was free to use it for certain purposes. Brief for United States 34–36. But an individual need not have “complete ownership or exclusive control” before he can assert a Fourth Amendment challenge against the search of real property. *Carpenter*, 585 U.S., at 401, 138 S.Ct. 2206 (GORSUCH, J., dissenting). Instead, we have long recognized, a “tenant[t] [or] resident family membe[r]” who does not enjoy “fee simple title” in a house has a sufficient interest in it to give rise to a Fourth Amendment right. *Ibid.* And I fail to see why the law should differ markedly when it comes to personal property. If you “[t]oss your keys to a valet at a restaurant” or “[a]sk your neighbor to look after your dog while you *2222 travel,” you may entrust your personal property to another and license him to do certain things with it, much as Mr. Chatrle did with his Location History data. *Id.*, at 399, 138 S.Ct. 2206. But that hardly means that property is no longer yours. *Ibid.*

Nor does it matter that those who wrote the Fourth Amendment might not have imagined an electronic diary or map of one's travels. As with other laws, the terms found in the Fourth Amendment carry their original public meaning and can bear more applications than its drafters might have expected or intended. See *id.*, at 400, 138 S.Ct. 2206. So just as the First Amendment protects speech over the internet today no less than it did speech delivered in the town square in 1791, it should hardly come as a surprise that the Fourth Amendment might protect as personal “effects” electronic diaries of one's travels as it always has more traditional ones. See *Kyllo v. United States*, 533 U.S. 27, 40, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (observing that a “search” of a home can take place not just by physical entry but also by the external use of thermal-imaging devices).

Because Mr. Chatrle's Location History data is his effect, it is subject to the Fourth Amendment's restrictions when the government searches it. So, was there a search? The government conducts a search when it “ ‘look[s] over or through for the purpose of finding something.’ ” *Id.*, at 32, 121 S.Ct. 2038, n. 1 (quoting N. Webster, *An American Dictionary of the English Language* 66 (1828) (reprint 6th ed. 1989)). Under our precedents, none of which the government asks us to overrule, a search equally transpires when government officials enlist private parties in that task. See *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 614, 109

S.Ct. 1402, 103 L.Ed.2d 639 (1989) (Fourth Amendment “protects against” searches “effected” by a private party “if the private party acted as an instrument or agent of the Government”). And that’s exactly what occurred here: The government conducted a search both when it compelled Google to rummage through Mr. Chatrie’s data at “step one,” and when it later examined that data for itself and demanded more data yet from Google at “step two.” See *ante*, at 2202 - 2203 (describing the stepwise process in which the searches were conducted in this case).

*

*

I might have hoped that the Court would have pursued a more traditional approach to the Fourth Amendment today. But look carefully and you will see hints of it at work even in the Court’s opinion. Why is the Court so protective of Location History data, email, and electronically stored photos and calendars? See *ante*, at 2212 - 2213. Because, it turns out, “a user reasonably understands” all those things “as his own.” *Ante*, at 2212 - 2213. Put another way, they are his effects. And why does the Court hold Mr. Chatrie’s effects protected by the Fourth Amendment even though a third party stores them? Because, the Court says, those effects remain his “even though [they are] stored on Google’s servers.” *Ibid*. Put another way, entrusting your effects to a third party for certain agreed purposes doesn’t mean they are no longer yours. While more work may lie ahead to bring coherence to our Fourth Amendment jurisprudence, perhaps this is a start.

Justice ALITO, with whom Justice THOMAS joins as to Part I and with whom Justice BARRETT joins as to Parts II–B, II–C–1, and II–C–2, dissenting.

Eight years ago, I warned that this Court’s decision in **2223 Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018), would produce one of two outcomes. Either the Court would need to clarify *Carpenter*’s limits in a future decision, or *Carpenter* would usher in “revolutionary developments” in our doctrine by giving criminal suspects a “protected Fourth Amendment interest in any sensitive personal information about them that is collected and owned by third parties.” *Id.*, at 385, 138 S.Ct. 2206 (ALITO, J., dissenting). Today, the Court takes the country down the latter path. In doing so, the Court sheds *Carpenter*’s self-

imposed boundaries and further destabilizes longstanding Fourth Amendment jurisprudence.

To make matters worse, the majority does all this in an advisory opinion. Although today’s decision will send seismic waves through our Fourth Amendment doctrine, not one iota of the majority opinion will affect the outcome of this case. The Court knows this and does not claim otherwise. Indeed, by refusing to review the one question that could have at least theoretically given Chatrie some hope of relief, the Court carefully set the stage for its planned performance: striking a pose as a great champion of privacy in the digital age. I cannot support this irresponsible escapade.

I

The Court should not have granted certiorari in this case, and under any faithful application of our precedents, it should now either dismiss this petition or affirm the decision below based on the “good-faith exception” to the exclusionary rule. Instead, the Court issues an advisory opinion concerning a now-obsolete “geofence” procedure. Last Term, the Court worried out loud about rushing in to judge “new technologies with transformative capabilities” that we barely understand. *TikTok Inc. v. Garland*, 604 U.S. 56, 62, 145 S.Ct. 57, 220 L.Ed.2d 319 (2025) (*per curiam*). In cases involving such technology, the Court proclaimed, we should take care not to “embarrass the future.” *Ibid*. (quoting *Northwest Airlines, Inc. v. Minnesota*, 322 U.S. 292, 300, 64 S.Ct. 950, 88 L.Ed. 1283 (1944)). Today, the Court exhibits no such modesty.

A

It has long been established that federal courts may not issue “advisory opinions” that do not bear on the rights of the litigants before them. *Lewis v. Continental Bank Corp.*, 494 U.S. 472, 477, 110 S.Ct. 1249, 108 L.Ed.2d 400 (1990). At the appellate stage, this principle means that courts should resolve only those questions on which a favorable ruling would provide a litigant redress from the judgment below. See *Food Marketing Institute v. Argus Leader Media*, 588 U.S. 427, 432–433, 139 S.Ct. 2356, 204 L.Ed.2d 742 (2019). The question on which the Court granted certiorari in this case cannot satisfy this requirement under any colorable view of the law. The Court should therefore decline to answer it.

Okello Chatrie's ongoing stake in this case stems from his conviction for robbing a bank and brandishing a firearm. On appeal, Chatrie challenged those convictions on only one ground. He argued that the District Court erred in denying his motion to suppress the fruits of the geofence procedure that led to his identification as the bank robber.¹ So, unless he can show that *2224 this evidence should be suppressed, he cannot obtain any relief. And his chances of making the showing needed to justify suppression are virtually zero.

The police obtained information about Chatrie's location at the time of the robbery pursuant to a warrant issued by a neutral magistrate. And when evidence is obtained under such a warrant, a defendant seeking suppression must overcome the good-faith exception to the exclusionary rule. *United States v. Leon*, 468 U.S. 897, 923, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). A majority of the Court of Appeals for the Fourth Circuit, sitting en banc, held that Chatrie could not do so. 136 F.4th 100, 101 (2025) (Diaz, C. J., concurring); *id.*, at 114 (Niemeyer, J., concurring); *id.*, at 115 (King, J., concurring); *id.*, at 115, n. 1 (Winn, J., concurring in judgment); *id.*, at 142 (Heytens, J., concurring). That holding suffices to affirm the District Court's admission of the geofence evidence and thus independently supports the Fourth Circuit's judgment. Accordingly, any review by this Court should concern an issue that could at least plausibly disturb that good-faith holding. Cf. *Stewart v. IHT Ins. Agcy. Group, LLC*, 990 F.3d 455, 457 (CA6 2021).

On this score, today's decision fails. The majority does not dispute the Fourth Circuit's good-faith analysis, and nothing in its opinion casts a shred of doubt on that holding. See *ante*, at 2204, n. 4. To overcome the good-faith exception, Chatrie would need to show that either (1) the affidavit supporting the geofence warrant was knowingly or recklessly false, (2) the magistrate rubber-stamped the warrant application, (3) the affidavit was “bare bones,” or (4) the warrant application was so facially deficient that no reasonable officer would rely on it. *Leon*, 468 U.S., at 923, and n. 24, 104 S.Ct. 3405. Yet nothing in the majority opinion touches on any of these matters. Thus, nothing in today's decision bears on the Fourth Circuit's good-faith holding. And because that holding independently supports the judgment below, the Court's opinion is advisory.²

This outcome was guaranteed as soon as this Court granted certiorari. When seeking review in this Court, Chatrie recognized that dislodging the Fourth Circuit's judgment required that he prevail on the good-faith issue, so his petition

asked us to alter the good-faith exception. See Pet. for Cert. i, 34–37 (asking the Court to create a *2225 carve-out to the good-faith exception). Yet the Court excluded the good-faith issue from its grant of certiorari, 607 U. S. 1148, — S.Ct. —, 223 L.Ed.2d 553, 2026 WL 120676 (2026), ensuring that any opinion would be advisory. Indeed, even if the Court were to decide that the warrant in this case was deficient, there would be no colorable argument on remand that all reasonable officers would have correctly predicted that outcome. See *Leon*, 468 U.S., at 923, 104 S.Ct. 3405. After all, this Court has never provided guidance on how to apply the Warrant Clause when the police request geolocation data from a third party. See *Carpenter*, 585 U.S., at 316–320, 138 S.Ct. 2206 (noting only that such a warrant requires probable cause). Accordingly, it would be nearly impossible for Chatrie to prove that the police here (and, by extension, every other officer who ever relied on this type of geofence warrant) acted in bad faith. See *Davis v. United States*, 564 U.S. 229, 240, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011) (Fourth Amendment violations “trigger the harsh sanction of exclusion only when they are deliberate ... and culpable”). In sum, no resolution of the question on which the Court granted certiorari could have disturbed the Fourth Circuit's good-faith holding and, thus, its judgment.

The Court therefore erred by granting certiorari, and we should now dismiss this petition as improvidently granted. See *Conway v. California Adult Authority*, 396 U.S. 107, 110, 90 S.Ct. 312, 24 L.Ed.2d 295 (1969) (*per curiam*) (dismissing when resolving the issue addressed in the petition would produce an advisory opinion). Alternatively, this Court could affirm the decision below on good-faith grounds. Although the Court did not grant certiorari on this question, we may affirm a judgment on any ground supported by the record, and we would not be the court of “first view” on the good-faith issue. *Upper Skagit Tribe v. Lundgren*, 584 U.S. 554, 560–561, 138 S.Ct. 1649, 200 L.Ed.2d 931 (2018). The Government properly presented this issue below, the District Court admitted the contested evidence on good-faith grounds, a majority of the en banc Fourth Circuit voted to affirm on that basis, and the Government continued to press good faith at the petition and merits stages in this Court. See Government's Response in Opposition to Defendant's Motion for Suppression, ECF Doc. 41, p. 21; 590 F.Supp.3d 901, 937 (ED Va. 2022); Brief in Opposition 13; Brief for United States 47–48. This Court therefore has every reason to affirm on that ground.

Instead, the Court charges forward to decide the question presented, even though the majority cannot discern any impact that its decision has on the Fourth Circuit's judgment. See *ante*, at 2204, n. 4. The majority thus issues a plainly advisory opinion, violating this Court's "oldest and most consistent" justiciability rule. *Flast v. Cohen*, 392 U.S. 83, 96, 88 S.Ct. 1942, 20 L.Ed.2d 947 (1968) (internal quotation marks omitted).

B

Advisory-opinion concerns aside, our prudential certiorari considerations further counseled against granting certiorari. Writs of certiorari are discretionary, and we reserve them for "compelling" cases in which the court below "has decided an important question of federal law." This Court's Rule 10. The question in this case does not qualify.

Chatrle's petition asked whether the geofence procedure that the police used here comports with the Fourth Amendment. The answer to this question has scarcely any ongoing significance. Google, the Government, and the majority all agree that Google has modified its Location *2226 History service in a manner that forecloses future use of this geofence procedure. *Ante*, at 2201, n. 2; Brief for Google LLC as *Amicus Curiae* 2; Brief for United States 42, n. 3. Chatrle does not offer any evidence to the contrary. See Tr. of Oral Arg. 17–18; Brief for Petitioner 5; Pet. for Cert. 10–11. As a result, Fourth Amendment challenges to this geofence procedure will likely pass into obscurity soon.

This Court has long been averse to granting certiorari on questions "that time [will] soon bury." *Darr v. Burford*, 339 U.S. 200, 227, 70 S.Ct. 587, 94 L.Ed. 761 (1950) (Frankfurter, J., dissenting). This aversion applies with special force here given this case's subject matter. The Fourth Amendment's application to surveillance technology turns on the "unique nature" of the technology involved and the way in which the police use it to collect information. *Carpenter*, 585 U.S., at 309, 138 S.Ct. 2206. For instance, when determining whether law enforcement's use of a technology requires a warrant or is otherwise "unreasonable," this Court has considered the technology's capabilities, prevalence, costliness, conspicuousness, intrusiveness, precision, accuracy, security, and comprehensiveness. See, e.g., *Kyllo v. United States*, 533 U.S. 27, 34–35, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001); *United States v. Jones*, 565 U.S. 400, 429–431, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012)

(ALITO, J., concurring in judgment); *Maryland v. King*, 569 U.S. 435, 446–465, 133 S.Ct. 1958, 186 L.Ed.2d 1 (2013); *Birchfield v. North Dakota*, 579 U.S. 438, 461–464, 136 S.Ct. 2160, 195 L.Ed.2d 560 (2016); *Carpenter*, 585 U.S., at 310–313, 138 S.Ct. 2206. Because these qualities vary from one technology to the next, the specific application of the Fourth Amendment does as well. Such variability renders this case all the less suitable for our review. Whatever one's jurisprudential views about the Fourth Amendment in the digital age, a case concerning a now-obsolete geofence procedure is an odd vehicle for pronouncing them.

None of this is to say that today's decision will be inconsequential. As the majority works its way through the question in this case, it makes sweeping proclamations with implications far beyond the specific procedure that the police used here. But this fact only underscores the advisory nature of today's decision. The majority has candidly little to say about the relevance of its decision for Chatrle's conviction. *Ante*, at 2204, n. 4. Instead, the Court uses this case as a vehicle to once again "make a statement about privacy in the digital age." See *Carpenter*, 585 U.S., at 386, 138 S.Ct. 2206 (ALITO, J., dissenting). Because that function is not a proper use of this Court's certiorari docket, we should not have granted this petition and should now dismiss it.

II

The Court's resolution of the merits of this case is equally flawed. Applying the Fourth Amendment to 21st-century investigation methods is undoubtedly an important and challenging task, and the Court ought to proceed cautiously. Yet the majority, faced with only countervailing authority in the first two centuries of this Court's case law, relies almost exclusively on our decision in *Carpenter*. And rather than moderate *Carpenter*'s departures from long-established Fourth Amendment law, the majority propels that decision's disruption to new heights.

A

If the Court were to apply the Fourth Amendment as understood for the first century of this Nation's history, we would find no "search" of Chatrle's papers or effects, much less an "unreasonable" one. *2227 Until the last decades of the 19th century, the Search and Seizure Clause protected only the physical security of one's person and property,

and document-production orders were not understood to be “searches.” See *Katz v. United States*, 389 U.S. 347, 367–374, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Black, J., dissenting); *Carpenter*, 585 U.S., at 348–357, 138 S.Ct. 2206 (THOMAS, J., dissenting); *id.*, at 363–372, 138 S.Ct. 2206 (ALITO, J., dissenting). Under those principles, Chatrrie's arguments are meritless.

To illustrate this point, imagine that Chatrrie spent his free time taking road trips across the United States. And suppose that he entered into a contract with a travel agency, under which the agency would provide him valuable information about places to visit and activities to try as he traveled from place to place. Suppose that the contract, in exchange for these services, authorized the travel agency to maintain a detailed chronicle of Chatrrie's adventures and to use that information to develop its business, expand its offerings, and advertise to prospective customers. If a grand jury had subpoenaed the travel agency for the records of Chatrrie's travels, he would have no basis to object on search-and-seizure grounds. At least through the late 19th century, compelled document-production orders were simply not “searches.”

Likewise, until *Carpenter*, this Court held that the Fourth Amendment protected a person's security in only his own papers and effects, not those of a third party. *Carpenter*, 585 U.S., at 328, 138 S.Ct. 2206 (Kennedy, J., dissenting); *id.*, at 342, 138 S.Ct. 2206; (THOMAS, J., dissenting); *id.*, at 379–385, 138 S.Ct. 2206 (ALITO, J., dissenting). Chatrrie's claim would therefore fail for a second reason: He possesses no property interest in the information that Google conveyed to the police. To be sure, Chatrrie claims a property right in Google's Location History files under a bailor-bailee relationship, and he claims that the execution of the geofence procedure transgressed those rights. This argument radically reconceptualizes the traditional understanding of property rights. Cf. C. Reich, *The New Property*, 73 Yale L. J. 733 (1964). And even if Chatrrie possessed a property right in the Location History files on Google's servers, the conduct of the police in this case did not infringe that right. The geofence procedure did not give the police access to the Location History files themselves. Rather, Google used the information contained in those files to generate a spreadsheet that summarized objective, historical facts about Chatrrie's (and others') location in the hour before and hour after the robbery. See Decl. of S. Rodriguez, ECF. Doc. 96–2, pp. 2–3; 107 F.4th 319, 324 (CA4 2024). The police sought and obtained those historical details, not the files on Google's servers. And whatever property rights Chatrrie might have

in the Location History files, he does not “own” historical facts about his movements in a given hour. If Chatrrie, instead of using Location History, had written and copyrighted a private memoir about his crimes, he would not have a Fourth Amendment claim if the police asked a proofreader whether Chatrrie was at the credit union during the robbery. Cf. *International News Service v. Associated Press*, 248 U.S. 215, 234, 39 S.Ct. 68, 63 L.Ed. 211 (1918) (distinguishing between having a property interest in a newspaper article and having a property interest in the historical facts set forth in the article). Chatrrie therefore cannot show that the police here transgressed any rights in his papers or effects.

In short, under traditional search-and-seizure principles, Chatrrie could not challenge the geofence procedure here under the Fourth Amendment.

***2228 B**

1

In the 20th century, this Court expanded its Fourth Amendment doctrine to protect more than the physical security of one's person and property. Beginning in *Katz*, the Court held that the Fourth Amendment also protects a person's “reasonable expectation of privacy” from government intrusions. 389 U.S., at 360, 88 S.Ct. 507 (Harlan, J., concurring); see also *id.*, at 351–353, 88 S.Ct. 507 (majority opinion).

Whatever one thinks of *Katz*'s expansion of Fourth Amendment doctrine, this Court at least had the prudence to tread cautiously when implementing that expansion. Indeed, the Court spent much of the 20th century emphasizing the limits of *Katz*'s reach. For instance, the Court held that *Katz* did not require the police to obtain a warrant for visual or physical surveillance outside a house's curtilage. *Oliver v. United States*, 466 U.S. 170, 178, 104 S.Ct. 1735, 80 L.Ed.2d 214 (1984). Nor could a defendant generally claim an “expectation of privacy” in someone else's home, his own public travels, his face-to-face conversations with another person, or information that he shared with a business. *Minnesota v. Carter*, 525 U.S. 83, 89–91, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998); *United States v. Knotts*, 460 U.S. 276, 281–282, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983); *United States v. White*, 401 U.S. 745, 751–752, 91 S.Ct. 1122, 28 L.Ed.2d 453 (1971) (plurality opinion); *Smith v. Maryland*, 442 U.S. 735, 744, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). If *Katz*

ushered in a revolution in Fourth Amendment doctrine, the Court was quick to cabin its impact. See also *New York v. Burger*, 482 U.S. 691, 693, 700, 107 S.Ct. 2636, 96 L.Ed.2d 601 (1987) (holding that *Katz* does not require a warrant for inspections of “pervasively regulated industries”); *California v. Greenwood*, 486 U.S. 35, 40–41, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988) (holding that *Katz* does not protect privacy interests in household garbage left curbside); *California v. Ciraolo*, 476 U.S. 207, 213–215, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) (holding that *Katz* does not require a warrant for aerial surveillance).

Similarly, even after *Katz*, the Court recognized that legislatures still bore primary responsibility for regulating the use of new technologies and investigation methods. Thus, when legislatures developed reasonable schemes to administer such activities, the Court was reluctant to constitutionalize additional rules. See, e.g., *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 534–539, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967) (upholding the constitutionality of a search conducted pursuant to “reasonable legislative or administrative standards”); *King*, 569 U.S., at 465, 133 S.Ct. 1958 (holding that a DNA collection scheme was constitutional in part because state statute regulated how records could be used); see also *Burger*, 482 U.S., at 707–711, 107 S.Ct. 2636 (allowing warrantless inspections pursuant to a regulatory scheme designed to combat modern problems with car theft). As much as *Katz* reflected a departure from traditional Fourth Amendment rules, this Court's decisions made clear that it was a measured one.³

S.Ct. 1619. Thus, when the defendant “voluntarily conveyed” his financial information to a bank by depositing money or cashing checks, he assumed the risk that the bank would create a paper trail of that information for its own business purposes. *Id.*, at 442, 96 S.Ct. 1619. The defendant likewise assumed the risk that the bank might share that information with others, including the police. *Ibid.* The Court therefore held that the defendant had no Fourth Amendment rights in the bank's records of his transactions.

What was true about the bank records in *Miller* is true about Location History here. Chatric voluntarily conveyed his location information to Google, and Google created a digital paper trail of that information. Like the bank in *Miller*, Google was no neutral custodian in this arrangement. *Id.*, at 440, 96 S.Ct. 1619. In exchange for allowing Chatric to use its Location History service, Google could use his location information for its own business purposes, such as sending Chatric location-targeted advertisements from third parties. 590 F.Supp.3d at 907–908. So, by giving Google his location information for its own use, Chatric assumed the risk that Google might disclose location information to others, including the police. *Miller*, 425 U.S., at 443, 96 S.Ct. 1619. Indeed, Google advises its users that the company could use their location information for its own advertising purposes and could share that information with law enforcement. *E.g.*, 1 App. 69–70. Thus, like the defendant in *Miller*, Chatric cannot now claim a reasonable expectation of privacy in those data. The police therefore would not need a warrant to perform the geofence procedure under our 20th-century precedents.

2

C

The geofence procedure in this case did not violate Chatric's Fourth Amendment rights under these 20th-century precedents. *2229 These precedents hold that a defendant does not have a reasonable expectation of privacy in records that a company generates by virtue of the defendant's use of its services. This rule has come to be known as the third-party doctrine. The Court articulated this rule in *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), holding that the police did not violate a defendant's Fourth Amendment rights when they obtained transaction records from his bank. In reaching this conclusion, *Miller* emphasized that a bank is not merely a neutral custodian of its customers' financial information, but rather a party to an ongoing business relationship with them. *Id.*, at 440–441, 96

1

Without any support in 19th- or 20th-century understandings of the Fourth Amendment, Chatric and the majority rely primarily on this Court's decision in *Carpenter*. *Carpenter* held that the police must obtain a warrant before ordering a cellular carrier to provide more than six days of cell-site records about a customer (*i.e.*, information about the specific cell towers to which a cell phone connected). 585 U.S., at 315–316, 138 S.Ct. 2206. Like *Katz*, *Carpenter* extended the Fourth Amendment's warrant requirement to encompass a category of government investigations that it had never previously covered. Before *Carpenter*, a criminal defendant who objected to police collection of cell-site records would

have faced at least two legal hurdles: the historical distinctions between searches and subpoenas *duces tecum*, and the third-party doctrine. *Carpenter*, 585 U.S., at 361–362, 138 S.Ct. 2206 (ALITO, J., dissenting). *Carpenter* thus reflected a “stark departure” from both traditional Fourth Amendment principles and this Court’s 20th-century doctrine. *Id.*, at 321, 138 S.Ct. 2206 (Kennedy, J., dissenting).

Nonetheless, *Carpenter* maintained that its departure from these doctrines was *2230 “narrow.” *Id.*, at 316, 138 S.Ct. 2206 (majority opinion). The question presented in *Carpenter* was whether the Fourth Amendment allows “the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days,” Pet. for. Cert. in *Carpenter v. United States*, O. T. 2017, No. 16–402, p. i, and the Court purported to resolve no more than the question before it, 585 U.S., at 316, and n. 4, 138 S.Ct. 2206. *Carpenter*’s analysis likewise anchored itself in the “unique nature” of the particular cell-site records that the police had collected in that case. *Id.*, at 315, 138 S.Ct. 2206. In “declin[ing] to extend” the third-party doctrine to weeks-long cell-site records, *Carpenter* highlighted various aspects of that dataset that, in the majority’s view, afforded the defendant a stronger expectation of privacy than the defendants in our earlier third-party precedents. *Ibid.*

Three of those aspects—duration, comprehensiveness, and voluntariness—deserve mention here. First, unlike traditional police-surveillance techniques, the dataset in *Carpenter* captured the “whole of [a person’s] physical movements” over 127 days, violating Americans’ reasonable expectation that they would not be “secretly monitor[ed]” for a “very long period.” *Id.*, at 310, 138 S.Ct. 2206 (internal quotation marks omitted). Second, the dataset gave the police an “all-encompassing record” of the defendant’s whereabouts that tracked him “beyond public thoroughfares and into private residences ... and other potentially revealing locales.” *Id.*, at 311, 138 S.Ct. 2206. Third, the Court determined that cell-phone users do not “voluntarily” share their cell-site information with cellular carriers in the same way that the defendant in *Miller* voluntarily conveyed his transaction information to a bank. *Carpenter*, 585 U.S., at 315, 138 S.Ct. 2206. The Court reasoned that because cell phones are “indispensable to participation in modern society” and “[v]irtually any activity on [a] phone” generates cell-site records, a person has no practical choice but to constantly convey this information to third parties. *Ibid.* Based on these aspects of the dataset at issue, *Carpenter* concluded that the

defendant had a strong enough privacy expectation that the rationale undergirding our third-party case law did not apply. *Id.*, at 314–315, 138 S.Ct. 2206. *Carpenter* therefore held that the police needed a warrant to obtain seven or more days of cell-site records from a cellular carrier. *Id.*, at 310, n. 3, 138 S.Ct. 2206.

2

Carpenter did not require the police to obtain a warrant for the geofence procedure here. By its own terms, *Carpenter*’s holding was keyed to the “unique nature” of the cell-site records in that case. *Id.*, at 309, 315, 138 S.Ct. 2206. *Carpenter* expressly left open the question whether the police would need a warrant for location data spanning less than a week, as is the case with the data here. *Id.*, at 310, n. 3, 138 S.Ct. 2206. *Carpenter* likewise declined to address situations where the police request information about all devices in a given area at the time of a crime (e.g., a geofence procedure), as opposed to continuous location information about one specific device. *Id.*, at 316, 138 S.Ct. 2206. For this reason alone, *Carpenter* does not dictate an outcome here.

Nor does *Carpenter*’s reasoning justify extending its holding to this case. Here, the police requested two pieces of information that could implicate Chatrie’s Fourth Amendment interests: (1) whether he was within 150 meters of the credit union during the robbery, and (2) if he was, where he traveled during the 1-hour periods immediately before and afterward. Along *2231 three of the dimensions that *Carpenter* found relevant, Chatrie has a far lesser privacy interest in this information than the defendant did in the records at issue in that case. The third-party doctrine therefore controls.

First, unlike the data collection in *Carpenter*, the geofence procedure in this case did not risk uncovering the “whole of [someone’s] physical movements.” 585 U.S., at 310, 138 S.Ct. 2206. In contrast to the 127 days of cell-site records in *Carpenter*, the request made by the police here spanned just two hours.⁴ Until today, this Court had recognized a Fourth Amendment difference between tracking a person’s movements for a “brief stretch” and cataloging them for an “‘extended period of time.’” *Ibid.*; *Jones*, 565 U.S., at 430, 132 S.Ct. 945 (opinion of ALITO, J.). Although it might be difficult to “identify with precision” the dividing line between these two durations, a 2-hour stint of location tracking is “surely” too limited to constitute the “all-encompassing record” that triggered heightened privacy

concerns in *Carpenter. Jones*, 565 U.S., at 430, 132 S.Ct. 945 (opinion of ALITO, J.); *Carpenter*, 585 U.S., at 311, 138 S.Ct. 2206.

Second, the limited geofence procedure here was far less likely to open “an intimate window” into Chatrle's “ ‘familial, political, professional, religious, and sexual associations’ ” than was the chronicle that the police obtained in *Carpenter. Id.*, at 311, 138 S.Ct. 2206. Whereas the procedure in *Carpenter* gave the police a comprehensive log of the defendant's movement everywhere he went, the geofence's boundaries here centered on a credit union,⁵ a public place where individuals lack a reasonable expectation of privacy.⁶ Cf. *Miller*, 425 U.S., at 442–443, 96 S.Ct. 1619 (holding that a person has no expectation of privacy in his dealings with a bank); *Knotts*, 460 U.S., at 281–282, 103 S.Ct. 1081 (holding that a person has no expectation of privacy in his travels through public places). To be sure, the geofence procedure also captured some people's movements outside the geofence in the hour before and after they visited the credit union, and it is feasible that some people might have traveled to a private location during that window. But the incidental acquisition of such information through otherwise-permissible surveillance does not violate Chatrle's Fourth Amendment rights. *Id.*, at 282, 103 S.Ct. 1081 (holding that no search of the defendant occurred when a police beeper monitored his travel from a public place to his private residence). Moreover, if the geofence procedure uncovered information about Chatrle's movements within a private location, the proper solution would be to suppress that information, rather than the fruits of the entire procedure. See *2232 *United States v. Karo*, 468 U.S. 705, 720–721, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984) (holding that location information from one leg of a defendant's journey in private places was the fruit of an unconstitutional search but upholding the use of location information from a different leg of that journey in nonprivate places).

Third, unlike the generation of cell-site records, the creation of Location History data is voluntary and not integral to a cell phone's functionality. Cell-site records are the by-product of every phone interaction with a cell tower and thus an unavoidable consequence of sending text messages, making phone calls, or connecting to the internet. *Carpenter*, 585 U.S., at 315, 138 S.Ct. 2206. A person can avoid creating those records only by forgoing all use of a cell phone for these purposes, and doing so would render useless this “indispensable” component of modern life. *Ibid.* In contrast, users need not enable Location History for their phones to

function as expected. That most Google accountholders carry on without using Location History is strong evidence that the service is not a “pervasive and insistent part of daily life” in the way that creating cell-site records is. *Ibid.* (internal quotation marks omitted); see *ante*, at 2213.

Thus, on the criteria that *Carpenter* found relevant in determining whether to apply the third-party doctrine, Chatrle has a far lesser privacy interest in the data that the police sought here. For that reason, I would not extend *Carpenter* here, and I would hold that the police did not need a warrant.

3

The majority reaches the opposite outcome, and in doing so, it announces a new rule of Fourth Amendment law: The police must obtain a warrant every time they access *any* cell-phone location information from a third party, however brief the duration, however innocuous the request, and however voluntarily that information was disclosed by the user. *Ante*, at 2213. This rule significantly extends *Carpenter* and repudiates the boundary lines that *Carpenter* drew to distinguish its novel holding from longstanding doctrine. Whereas *Carpenter* rested its holding on the difference between obtaining a “brief stretch” of location information and receiving a chronicle spanning a week or more, 585 U.S., at 310, 315, 138 S.Ct. 2206, the majority holds that the police need a warrant regardless of the duration of the data sought, *ante*, at 2208 - 2212. Whereas *Carpenter* rested its holding on the concern that an all-encompassing dataset would reveal a defendant's presence in sensitive locations, 585 U.S., at 311, 138 S.Ct. 2206, the majority holds that the police need a warrant regardless of whether a geofence captures any sensitive locations, *ante*, at 2211 - 2212. Whereas *Carpenter* rested its holding on the near-universal use of cellphones and the unavoidability of generating cell-site records, 585 U.S., at 315, 138 S.Ct. 2206, the majority holds that the police need a warrant regardless of how widespread a technology is or how feasibly users may opt out, *ante*, at 2213 - 2215. Now, we are told, all that matters is whether a given investigative procedure enables the police to obtain location information easily using a technology that did not exist in “an earlier age.” *Ante*, at 2207 - 2209. If so, the police need a warrant.

This unshackling of *Carpenter* will unleash the very upheaval in Fourth Amendment law that *Carpenter* disclaimed. See 585 U.S., at 319, 138 S.Ct. 2206 (stating that its holding would apply “only ... in the rare case”). Today's decision

makes clear that the last two centuries of Fourth Amendment search doctrine simply do not apply to digital-age methods of tracking a *2233 suspect's location. And although the Court frames its holding as concerning only "location information," *ante*, at 2215, that qualification "might as well be written on the dissolving paper sold in magic shops," *Fulton v. Philadelphia*, 593 U.S. 522, 551, 141 S.Ct. 1868, 210 L.Ed.2d 137 (2021) (ALITO, J., concurring in judgment). If past is prologue, the parchment limits on today's holding will fade away just as quickly as *Carpenter*'s have.

4

In support of its sweeping conclusion, the majority argues that a duration-based or procedure-by-procedure approach to the Fourth Amendment would generate a "host of line-drawing questions." *Ante*, at 2210, n. 9; see also *ante*, at 2213 - 2215. I do not disagree, but those questions are the inevitable byproduct of the lines that *Carpenter* drew when it distinguished away longstanding doctrine. See 585 U.S., at 322, 339, 138 S.Ct. 2206 (Kennedy, J., dissenting) (explaining that *Carpenter* drew an "unprincipled and unworkable line" and imposed an "arbitrary 6-day cutoff"). Indeed, the majority's rejection of such line-drawing only betrays its expansion of *Carpenter*'s holding.

In any event, the majority's approach creates its own share of line-drawing problems. What dividing line can explain why a defendant has a reasonable expectation of privacy in his cell-phone location information but not in his bank records? See *Miller*, 425 U.S., at 442-443, 96 S.Ct. 1619. Debit and credit cards might be viewed as comparably "indispensable to participation in modern society," and their use creates a detailed paper trail. *Carpenter*, 585 U.S., at 315, 138 S.Ct. 2206. As a result, modern bank records contain similarly comprehensive accounts of Americans' private lives, including "the political and religious organizations to which they donate; whether they have visited a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center; [and] whether they go to gay bars or straight ones." *Id.*, at 337, 138 S.Ct. 2206 (Kennedy, J., dissenting). But as long as *Miller* remains good law, see *Carpenter*, 585 U.S., at 316, 138 S.Ct. 2206 (majority opinion), the Fourth Amendment does not require the police to obtain a warrant for these records.⁷

More broadly, where does the boundary between *Carpenter* and the third-party doctrine lie after today? *Carpenter* gave "courts and law enforcement officers no indication how to determine whether any particular category of information falls" on the *Carpenter* or *Miller* side of the line, and today's decision does no better. *Carpenter*, 585 U.S., at 340, 138 S.Ct. 2206 (Kennedy, J., dissenting). Do the police need a warrant to obtain a person's Amazon purchase history? What about a person's Google search history or Venmo transaction log? Those kinds of information fall squarely within the third-party doctrine, and today's holding about "cell phone location information" does not ostensibly disturb that fact. *Ante*, at 2215 (internal quotation marks omitted). At the same time, those data can paint a similarly detailed picture of a person's private life, and law enforcement had no easy way to obtain this information in "an earlier age."⁸ *2234 *Ante*, at 2207 - 2209. If the Court maintains its unwillingness to engage with such "line-drawing questions," *ante*, at 2210 n. 9, *Carpenter*'s warrant requirement might soon come for all forms of digital surveillance.

* * *

In *Carpenter*, I worried that we might be "picking up the pieces" of our Fourth Amendment doctrine for a long time to come. 585 U.S., at 362, 138 S.Ct. 2206 (dissenting opinion). Today's decision all but guarantees that we will be cleaning up debris for the foreseeable future.

Justice BARRETT, dissenting.

I have no quarrel with *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018), or with the Court's decision to grant certiorari in this case. But I agree with Justice ALITO that under our Fourth Amendment precedent, including *Carpenter*, Chatrie had no reasonable expectation of privacy in data about his public movements that he voluntarily disclosed to Google. I therefore respectfully dissent.

All Citations

609 U.S. ----, 146 S.Ct. 2193, 225 L.Ed.2d 793, 2026 Daily Journal D.A.R. 5330, 31 Fla. L. Weekly Fed. S 984

Footnotes

- ^x The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Timber & Lumber Co.*, 200 U.S. 321, 337, 26 S.Ct. 282, 50 L.Ed. 499.
- 1 Throughout this opinion, we describe how Location History worked at the time the warrant at issue was executed. As noted below, Google has since then instituted a significant change, which apparently insulates Location History data from geofence warrants. See *infra*, at 2201, n. 2.
- 2 Except that in July 2025, years after the geofence warrant used in this case, Google made a change: It now stores Location History data on individual users' devices rather than on its own servers. See Brief for Google LLC as *Amicus Curiae* 2. Google represents that, as a result, it is no longer capable of responding to geofence warrants that seek Location History data. See *ibid.*
- 3 Google is not the only tech company that has received geofence warrants; so have Apple, Lyft, Snapchat, and Uber, among others. See 136 F.4th 100, 102, n. 1 (CA4 2025) (en banc) (Diaz, C. J., concurring). But Google is the “most common recipient and the only one known to respond.” *Ibid.*
- 4 In line with our grant of certiorari, we do not address whether the good-faith exception to the exclusionary rule still allows the admission of the Location History data in this case. That question remains for the Fourth Circuit to consider anew, gleaning anything it thinks relevant from our decision on the substantive Fourth Amendment issues.

The principal dissent seeks to rehash our limited grant of certiorari, but we see no reason to doubt it. We have Article III jurisdiction in this case, as even the dissent concedes. See *post*, at 2224, n. 2 (ALITO, J.). That is because the Fourth Circuit is free to revisit the exclusionary rule issue in light of our opinion and to provide Chatrie with relief. See *Chafin v. Chafin*, 568 U.S. 165, 172, 133 S.Ct. 1017, 185 L.Ed.2d 1 (2013) (Article III jurisdiction disappears only when it becomes “impossible for the court to grant any effectual relief whatever to the prevailing party”). So what does the dissent mean when it continually labels this opinion “advisory” (*post*, at 2222 - 2223, 2223, 2224 - 2225, 2225, 2225 - 2226, 2226)—a term customarily used to describe opinions lacking a jurisdictional basis? Apparently, the dissent's objection is that we today decide a question involving the Fourth Amendment when the odds are strong (so says the dissent) that the Fourth Circuit will eventually, as it did before, resolve this case on exclusionary rule grounds. But to repeat, the Fourth Circuit may now consider anew, after review of our opinion, how the good-faith exception applies here. And the very decision establishing that exception held that courts should feel free to “resolv[e] the Fourth Amendment issue” before the good-faith issue, either to better assess good faith or “to guide future action by law enforcement officers and magistrates.” *United States v. Leon*, 468 U.S. 897, 925, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). So contra the dissent, there is nothing advisory (or otherwise improper) in today deciding the Fourth Amendment issue on which we previously granted certiorari.

- 5 The dissent suggests that this Court has tried to curtail *Katz* ever since deciding it, see *post*, at 2227 - 2229 (ALITO, J.); more energetically, the concurrence advocates overthrowing *Katz* and reverting to a solely property-based approach, see *post*, at 2218 - 2219, 2220 (GORSUCH, J., concurring in judgment). But this Court has faithfully applied *Katz* for some 60 years. Our decision in *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018), responded to the same arguments made today (see, e.g., *id.*, at 391-397, 88 S.Ct. 507 (GORSUCH, J., dissenting)) by reaffirming that *Katz* had “discredited the premise that property interests control” and that “privacy interests do not rise or fall with property rights.” 585 U.S., at 304, n. 1, 138 S.Ct. 2206. And in saying as much, *Carpenter* had plenty of other decisions to cite. See, e.g., *United*

exclusive test”); *Kyllo v. United States*, 533 U.S. 27, 32, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (stating that the Court has “decoupled violation[s] of a person's Fourth Amendment rights from trespassory violation of his property”). Of course, sometimes the privacy and property approaches will “align,” and an opinion adopting the one will resemble, in whole or part, an opinion adopting the other. *Florida v. Jardines*, 569 U.S. 1, 13, 133 S.Ct. 1409, 185 L.Ed.2d 495 (2013) (KAGAN, J., concurring). That is not because the privacy-based approach is groping toward the more “coheren[t]” property-based one, as the concurrence suggests. *Post*, at 2222 (GORSUCH, J.). It is simply because property law “naturally enough influence[s]” our “shared societal expectations” of what places and things count as private and should be free from governmental intrusion. *Georgia v. Randolph*, 547 U.S. 103, 111, 126 S.Ct. 1515, 164 L.Ed.2d 208 (2006); see *Carpenter*, 585 U.S., at 304, n. 1, 138 S.Ct. 2206 (“[P]roperty rights are often informative” in “determining which expectations of privacy are legitimate”). And when such an alignment of the two approaches occurs, then all the better.

- 6 An overlapping set of five Justices decided the case on a different ground, based on the Government's physical trespass of the vehicle. See *Jones*, 565 U.S., at 404–405, 132 S.Ct. 945.
- 7 A significant fraction of the dissent is devoted to relitigating *Carpenter*, from which its author dissented. See *post*, at 2222 - 2223, 2226 - 2228, 2229 - 2230, 2222 - 2234 (ALITO, J.). *Carpenter*, the dissent complains today, “extended the Fourth Amendment's warrant requirement to encompass a category of government investigations that it had never previously covered”: The decision “thus reflected a stark departure from both traditional Fourth Amendment principles and this Court's 20th-century doctrine.” *Post*, at 2229. In leveling that charge, the dissent re-ups arguments, point-for-point, that *Carpenter* specifically rejected. Compare *post*, at 2226 - 2227, 2229 - 2230 (maintaining that compelled document-production orders are never searches), with 585 U.S., at 317–318, 138 S.Ct. 2206 (rejecting that view); compare also *post*, at 2227, 2229 - 2230 (contending that the Fourth Amendment never protects documents held by third parties), with 585 U.S., at 313–316, 138 S.Ct. 2206 (likewise rejecting that view). In light of that outlook, it is perhaps not so surprising that the dissent criticizes today's decision as “rely[ing] primarily” on *Carpenter*, rather than on earlier Fourth Amendment decisions. *Post*, at 2229 - 2230. But on that supposed offense, we plead guilty as charged. *Carpenter* is the most recent decision of this Court to consider the Fourth Amendment's application to new surveillance technologies—indeed, to law enforcement's use of those technologies to create a “chronicle of [a cell-phone] user's past movements.” 585 U.S., at 300, 138 S.Ct. 2206. What would be grounds for complaint is if this decision did *not* “rely primarily” on *Carpenter*. *Post*, at 2229 - 2230. And as the next section of this opinion shows, the more one delves into the technologies at issue, the closer the parallels become. See *infra* this page and 2208 - 2209.
- 8 In comparing *Carpenter* and this case, the dissent sometimes treats the former as involving not 7 days but instead 127 days of location data. See *post*, at 2229 - 2230, 2230, 2230 - 2231 (ALITO, J.). But there is no basis for doing so. To be sure, one of the two wireless carriers involved in the case had turned over 127 days of data, as the Court noted. See 585 U.S., at 302, 138 S.Ct. 2206. But the other was ordered to turn over only 7 days, and the Court could not have been clearer that its holding applied whenever the Government accessed a week or more of CSLI data (with everything below that amount reserved). See *id.*, at 310, n. 3, 138 S.Ct. 2206 (“It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search”). The dissent acknowledges that fact (*post*, at 2231, n. 4), even as it repeatedly invokes the 127-day figure to make its comparative argument sound stronger.
- 9 The Government's grace-period approach to Fourth Amendment protection would also create a host of line-drawing questions. At what point, exactly, would a non-search become a search? In two hours, or six hours, or one day, or six days? And how often would the clock reset? If, say, the limit was six hours, could an officer request location data from 6 a.m. to noon, and then again from 12:30 to 6:30 p.m.? And if there were concurrent federal and state investigations of a crime, as there could have been here, would law enforcement access to Location History data double? The approach the Government offers would “keep defendants and

judges guessing for years to come.” *Riley v. California*, 573 U.S. 373, 401, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014).

- 10 The dissent replies that the “limited geofence procedure” authorized by the warrant here distinguishes this case from *Carpenter* because “the geofence’s boundaries” centered on “a public place.” *Post*, at 2231 (ALITO, J.). But as an initial matter, those boundaries were defined by a warrant. If accessing Location History does not count as a Fourth Amendment search, as the dissent generally suggests (see, e.g., *post*, at 2229, 2231 - 2232), there will not be a warrant (or any other means) to limit the scope of what law enforcement can demand. And even putting that aside, the dissent’s argument is wrong because it ignores how this geofence warrant actually worked. The geofence was not limited to the bank; it also included a nearby church. 590 F.Supp.3d 901, 918 (ED Va. 2022); cf. Brief for Google LLC as *Amicus Curiae* 12 (noting that, in Google’s experience, it is “common for a geofence to cover private homes, apartment buildings, ... hotels, [and] places of worship”). And regardless, the Location History data the police obtained at the second stage of the search process was not constrained by the geofence. In fact, it showed individuals’ trips to private residences, a school, and a hospital. See 590 F.Supp.3d at 923–924. So the geofence’s boundaries do not somehow turn Location History into a public-movements-only technology or ensure a less “comprehensive” log than in *Carpenter*. *Post*, at 2231.
- 11 Our precedents recognize exceptions to that rule—most prominently, “when the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable.” *Carpenter*, 585 U.S., at 319, 138 S.Ct. 2206. Today’s decision does not call into doubt, in such circumstances, a warrantless geofence search. See *id.*, at 320, 138 S.Ct. 2206 (noting the same for “warrantless access to CSLI”).
- 1 The majority characterizes the issue as whether the Government may introduce the location information that the police obtained through the geofence procedure. But Chatrrie also sought to suppress all the fruits of that location information, and these could potentially include a firearm matching one used in the crime, nearly \$100,000 of currency in bands bearing the bank teller’s signature, and his confession to the crime. See Defendant’s Motion to Suppress in No. 3:19–cr–00130 (ED Va.), ECF Doc. 29; Statement of Facts, ECF Doc. 229, p. 3.
- 2 I do not contend that the Court lacks Article III jurisdiction over this case as a formal matter. Chatrrie’s conviction suffices to render this litigation a “case or controversy,” regardless of the question on which the Court granted certiorari. The majority opinion is nonetheless advisory—not because I think “the odds are strong” that Chatrrie will lose on remand, contra, *ante*, at 2204, n. 4., but because the majority opinion does not disturb the basis for the Fourth Circuit’s judgment and thus Chatrrie’s conviction. This Court’s longstanding policy against issuing advisory opinions on constitutional issues is not limited to cases where we lack jurisdiction. See, e.g., *Rescue Army v. Municipal Court of Los Angeles*, 331 U.S. 549, 568, 67 S.Ct. 1409, 91 L.Ed. 1666 (1947) (holding that the Court possessed jurisdiction over a case but nonetheless declining to exercise it because the Court’s policy against issuing gratuitous constitutional opinions “has not been limited to jurisdictional determinations”); *Liverpool, New York & Philadelphia S. S. Co. v. Commissioners of Emigration*, 113 U.S. 33, 39, 5 S.Ct. 352, 28 L.Ed. 899 (1885) (“In the exercise of [its] jurisdiction, [this Court] is bound ... never to anticipate a question of constitutional law in advance of the necessity of deciding it”). An opinion composed exclusively of dicta is no less advisory simply because the Court has jurisdiction to pronounce such dicta.
- 3 Contrary to the Court’s characterization of my argument, *ante*, at 2205, n. 5, my purpose in recounting the developments in this Court’s post-*Katz* case law is to contrast the Court’s modesty during that period with its maximalist extension of *Carpenter* today.

- 4 In accurately noting that the data at issue in *Carpenter* spanned 127 days, I do not dispute that *Carpenter* drew the constitutional line at seven days. It is the majority that eschews *Carpenter*'s 7-day line. *Ante*, at 2208 - 2212.
- 5 The geofence also encompassed a nearby church, but Chatrrie has not claimed an expectation of privacy in that church. The church therefore has no bearing on whether the geofence procedure in this case violated *his* Fourth Amendment rights, and Chatrrie may not vicariously assert others' rights in support of his suppression motion. See *Rakas v. Illinois*, 439 U.S. 128, 148–150, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978).
- 6 The majority correctly notes that under my interpretation of *Carpenter*, the police could use a geofence procedure without obtaining a warrant in many situations. *Ante*, at 2211, n. 10. Contrary to the majority's suggestion, however, that fact does not mean that geofence procedures would lack any limits. Under *Carpenter*, if the police request and obtain sensitive, involuntarily collected location information that spans a week or more, they would still require a warrant.
- 7 One is left wondering on which side of the line location data from a mobile-payment service like Apple Pay falls.
- 8 Moreover, it is common these days for a single company, such as Google, to offer cellular plans, provide location services, maintain payment systems, host shopping platforms, and more. Companies have incentives to aggregate a user's data across these services, and this tendency will further complicate any efforts to draw Fourth Amendment lines among different sorts of third-party records.

End of Document

© 2026 Thomson Reuters. No claim to original U.S. Government Works.