ON REHEARING EN BANC

PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 22-4489

UNITED STATES OF AMERICA,

Plaintiff − Appellee,

v.

OKELLO T. CHATRIE,

Defendant – Appellant.

THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS; AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA; EIGHT FEDERAL PUBLIC DEFENDER OFFICES WITHIN THE FOURTH CIRCUIT; TECHNOLOGY LAW AND POLICY CLINIC AT NEW YORK UNIVERSITY SCHOOL OF LAW; ELECTRONIC FRONTIER FOUNDATION,

Amici Supporting Appellant.

PROJECT FOR PRIVACY AND SURVEILLANCE ACCOUNTABILITY, INC.,

Amicus Supporting Rehearing Petition.

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: January 30, 2025 Decided: April 30, 2025

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

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

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

Judge Gregory wrote a dissenting opinion.

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

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

PER CURIAM:

The judgment of the district court is

AFFIRMED.

DIAZ, Chief Judge, concurring:

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

This is such a case.

I.

A.

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

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

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

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

---

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.

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

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

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

B.

The police charged Chatrie with two crimes related to a bank robbery based on information obtained from Google through a geofence warrant. Detective Joshua Hylton prepared the warrant, which "drew a geofence with a 150-meter radius—with a *diameter* of 300 meters, longer than three football fields—in an urban environment." *Id.* at 918. That radius included the bank and a nearby church. *Id.* The warrant "sought location data for every device present within the geofence" for an hour around the time of the robbery (i.e., thirty minutes before and thirty minutes after). *Id.* at 919.

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

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

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

After his arrest, Chatrie, who had opted to share his Location History with Google, moved to suppress the location information, arguing that the warrant violated the Fourth Amendment. The district court agreed that *this* geofence warrant "plainly violate[d]" the

Constitution,[3] *id.* at 905, but nonetheless declined to suppress it under the good-faith exception to the Fourth Amendment, *id.* at 936–41.

The district court emphasized that "evidence obtained pursuant to a search warrant issued by a neutral magistrate need not be excluded if the officer's reliance on the warrant was 'objectively reasonable.'" *Id.* at 937 (cleaned up). Ticking through the factors the Supreme Court outlined in *United States v. Leon*, 468 U.S. 897 (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 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

[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.

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 (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 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.*

[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. "The first set of cases"—including *United States v. Knotts*, 460 U.S. 276 (1983), and *United States v. Jones*, 565 U.S. 400 (2012)—"address[ed] a person's expectation of privacy in his physical location and movements." *Carpenter*, 585 U.S. at 306–07. "In a second set of decisions"—including *Smith v. Maryland*, 442 U.S. 735 (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.

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 (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.[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 (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; *see also id.* at 315 (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 ("A cell phone

[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).

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

The balance, ever so delicate, swings from law enforcement and public safety to liberty and privacy interests depending on the record facts. Yet despite a shallow well of information and legal authority and a litany of unanswered questions as to our decision's

[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].

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 (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 (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).

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

[7] *See, e.g.*, *Ashwander v. Tenn. Valley Auth.*, 297 U.S. 288, 347 (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 (2011) ("In general, courts should think hard, and then think hard again, before turning small cases into large ones.").

> 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 (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 (1979), in which the magistrate became "a member, if not the leader, of the search party which was essentially a police operation," *id.* at 327, 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 previous guidance he had been given, which is, as my colleague explains, "what we expect reasonable officers to do when faced with such uncertainty." Opinion of HEYTENS, J., at 87 (concurring). Magistrates and prosecutors had approved three of Hylton's "mostly similar" prior warrants—"all but one [of which] incorporated a roughly 150-meter radius."

[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.

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 (1978) ("Search warrants are not directed at persons; they authorize the search of 'places' and the seizure of 'things,' and as a constitutional matter they need not even name the person from whom the things will be seized." (cleaned up)).

Take *Zurcher v. Stanford Daily*, 436 U.S. 547, 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. 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; *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, 145 S. Ct. 57, 62 (2025) (per curiam) (cleaned up).

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

But what guidance have my colleagues given today? Instead of a Fourth Amendment compass, we've gifted law enforcement (and the public) a labyrinth of—by my count, nine—advisory opinions, many pointing in different directions.[9] *See, e,g.*, *Riley v. California*, 573 U.S. 373, 398 (2014) (expressing a "preference" for "provid[ing] clear guidance to law enforcement" under the Fourth Amendment); Felix Frankfurter, *A Note on*

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

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 (1996) (Souter, J., concurring).

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

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

I.

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

There are many good reasons why the Supreme Court did not discard the third-party doctrine for all location data requests. Of course the concern for privacy in all of its dimensions was central to the Framers' contemplation. But the Fourth Amendment, to state the obvious, calls also for a balance between individual privacy and public safety. Favoring one over the other is at odds with the textual "touchstone" of the Amendment, which is reasonableness. *See Maryland v. King*, 569 U.S. 435, 448 (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 (2018). Not less, of course. But also not more.

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

II.

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

One, this restraint on investigative tools would frustrate law enforcement's ability to keep pace with tech-savvy criminals. Lawless actors of all kinds are growing more sophisticated and leveraging new technologies to commit crimes and evade detection. Transnational criminal organizations rely on digital currencies and encrypted communications to conceal their violence and fraud. 2023 WHITE HOUSE STRATEGY TO COMBAT TRANSNATIONAL ORGANIZED CRIME 3–4, 21 (2023). Terrorists likewise deploy emerging technologies like encryption, biotechnology, and artificial intelligence. Ian Moss,

U.S. Dep't of State, *Opening Remarks on Addressing Emerging Technology in the Realm of Racially or Ethnically Motivated Violent Extremism* (Feb. 14, 2024). Even small-time pimps encrypt their devices to block lawful access to their databases of sex-trafficking victims. *See Lawful Access*, Office of Legal Policy, U.S. Dep't of Justice (Nov. 18, 2022). Examples abound. In this age of innovation, those who would break the law spare no expense to employ the latest and greatest technological tools.

All the while, under appellant's view, local, state, and federal officers would lose the tools they need to protect the public from the modern-day criminal. More cold cases would go unsolved. Think of a murder where the culprit leaves behind his encrypted phone and nothing else. No fingerprints, no witnesses, no murder weapon. But because the killer allowed Google to track his location, a geofence warrant can crack the case. *See* Damien Christopher & Nick Penzenstadler, *Cold Cases Cracked by Cellphones: How Police Are Using Geofence Warrants to Solve Crimes*, USA TODAY (Sept. 8, 2022). Taking this tool of last resort out of law enforcement's hands would leave these case files collecting dust. The Fourth Amendment does not require allowing criminals to take advantage of cutting-edge technologies while preventing the government from doing the same. Technology enables the lawbreaker. Courts disable the government. This imbalance will only grow with time.

Two, law enforcement under appellant's view would be robbed of valuable channels of communication with the private sector. This case is a good example of those channels at work. Chatrie, like one-third of Google users, signed up for a program that shared his location data with Google. In return he got a "virtual journal of his past travels" and "real-

time traffic updates." *United States v. Chatrie*, 107 F.4th 319, 322 (4th Cir. 2024), *panel opinion vacated by order of the en banc court* (Nov. 1, 2024). And because he brought his phone to the robbery, the government was able to place Chatrie at the crime scene with Google's help.

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

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

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

III.

There is a further difficulty with categorically invalidating geofence warrants, namely that of extending the exclusionary rule with no regard to its costs. In *Hudson v. Michigan*, 547 U.S. 586 (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. 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. A reflexive expansion

of the exclusionary rule ignores the primary allegiance of courts to probative evidence and neglects the Supreme Court's clear instructions in *Hudson*.

The creation of remedies involves the weighing of costs and benefits, which often falls within the domain of legislators. Indeed, legislatures routinely enact laws balancing the competing considerations of personal privacy and public safety. For instance, the Electronic Communications Privacy Act, Pub. L. No. 99–508, 100 Stat. 1848 (1986), authorizes the government to collect people's communications and digital data for law enforcement purposes. But the law offers a *range* of procedural safeguards—anything from an administrative subpoena to a court-issued warrant based on probable cause—and remedies depending on the nature of the data. This type of compromise is a classic legislative task. Applying the exclusionary rule categorically to geofence warrants preempts legislative input in an area whose real impact upon the body politic would seem to invite some measure of popular participation.

IV.

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

The facts of this case are illustrative. Chatrie terrorized the employees and patrons of the Call Federal Credit Union in Midlothian, Virginia. He walked into the bank armed

with a handgun, told the teller that he had accomplices outside and that he was holding her family hostage, and threatened to "hurt[] everyone in sight" if she called the cops. *United States v. Chatrie*, 590 F. Supp. 3d 901, 905–06 (E.D. Va. 2022). Brandishing his gun, he forced everyone to the ground and ordered the manager to empty the safe. Chatrie was able to escape with $195,000. Because he was not apprehended at the scene, he eluded law enforcement for months. Officers were out of traditional leads. Only the geofence warrant eventually allowed police to track Chatrie down and restore a sense of resolution to the community. Without geofence location data, crimes even more serious than this one will escape detection.

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

Crime invades privacy. Crime limits freedom and narrows space. The fact that the Fourth Amendment exists to check the undeniable excesses of the modern state does nothing to diminish the fact that crime imperils the very values the Fourth Amendment exists to protect. The Framers resolved this dilemma by making reasonableness the Amendment's touchstone. It is dispiriting that some would proceed with nary a thought

given to that two-sided balance which reasonableness above all denotes. It will never do to see the future with but a single eye.

NIEMEYER, Circuit Judge, concurring:

I am pleased to join the opinions of Judge Wilkinson and Judge Richardson in full. Today's Fourth Amendment caselaw often starts with a pre-Internet analogy. *See Carpenter v. United States*, 585 U.S. 296, 306 (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 (1967); *id.* at 361 (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. 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. 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.

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

Of course, if a person were careful not to leave footprints, fingerprints, shell casings, or other markers behind, law enforcement would have to turn to other techniques and strategies to advance its investigation. But when such markers are left behind, law enforcement should not be denied the benefit of the person's carelessness when solving a crime. And *Carpenter* says nothing to the contrary. What *Carpenter* does say is that law enforcement needs to obtain a warrant before it utilizes digital technology to track a citizen's long-term movements — "the whole of his physical movements" — at least when that person is, in effect, compelled to leave behind a digital footprint wherever he goes.

585 U.S. at 313, 315; *see also United States v. Jones*, 565 U.S. 400, 430 (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 (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 (1979); *United States v. Miller*, 425 U.S. 435, 443 (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. 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 (1984).

KING, Circuit Judge, concurring:

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

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

The surveillance technologies at issue in this case—the very same ones that seem to thrill my colleagues who join Judge Wilkinson's separate opinion—would have been unimaginable to the Founders. Yet, in *Carpenter v. United States,* 585 U.S. 296 (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 (1983) (White, J., concurring)); *see United States v. Leon*, 468 U.S. 897, 925 (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. 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*.

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

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. The modern rule—adapted from Justice Harlan's concurring opinion in *Katz v. United States*, 389 U.S. 347 (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 (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. 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 (1979), and *United States v. Miller*, 425 U.S. 435 (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. And in *Miller*, police accessed the suspect's bank records, such as checks and deposit slips. *Miller*, 425 U.S. at 437–38. 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; *Miller*, 425 U.S. at 440–43; *Carpenter*, 585 U.S. at 308–09 (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 (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. 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.

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. The Court stressed that the beeper merely "augment[ed]" the officers' own "sensory faculties." *Knotts*, 460 U.S. at 282. 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 (quoting *Knotts*, 460 U.S. at 283–84).

The Court distinguished *Knotts* in *United States v. Karo*, 468 U.S. 705 (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. 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. 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.

In short, *Smith*, *Miller*, *Knotts*, and *Karo*—all decided before 1985—recognized that there is no reasonable expectation of privacy in simple records voluntarily conveyed to third parties in the ordinary course of business, or in one's short-term public movements. But as new surveillance technologies "enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 585 U.S. at 305 (quoting *Kyllo v. United States,* 533 U.S. 27, 34 (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. 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. "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 (quoting *Kyllo*, 533 U.S. at 35).

Next, in *United States v. Jones*, 565 U.S. 400 (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. *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. 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 (Sotomayor, J., concurring); *id.* at 418–31 (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 (Sotomayor, J., concurring); *id.* at 429–30 (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 (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 (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 (quoting *Illinois v. Lidster,* 540 U.S. 419, 426 (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. 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 (citation omitted).[2]

Two years later, the Court held in *Riley v. California*, 573 U.S. 373 (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. The Court recognized that digital storage compiles personal information of unprecedented volume, variety, and retrospectivity into a single

[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. 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.*.

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.

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

B.

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

Instead of "mechanically applying the third-party doctrine," *id.* at 314, *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.

[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 (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").

Based on those four considerations, the Court concluded that police access to CSLI violates reasonable expectations of privacy. *Id.* at 313.

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. 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.

II.

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

[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

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. 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).

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, ranging from "a dozen" to "several hundred" city blocks in size, which can be "up to 40

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

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

times more imprecise" in rural areas, *id.* at 324 (Kennedy, J., dissenting). But Location History can locate a user within *meters*—and can even measure elevation, identifying the specific floor in a building where a person might be. *United States v. Chatrie,* 590 F. Supp. 3d 901, 908–09 (E.D. Va. 2022). Moreover, the CSLI collected in *Carpenter* was only recorded when a user placed or received a call—no call, no data. *Carpenter*, 585 U.S. at 302. 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. 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, 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. CSLI allowed police to "travel back in time" to "reconstruct a person's movements," unlocking "a category of information otherwise unknowable." *Id.* And because CSLI tracking "runs against everyone," "police need not even know in advance whether they want to follow a particular individual, or when." *Id.* "Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years." *Id.*

Location History data raises similar concerns. Google begins collecting Location History the moment the feature is enabled and retains it indefinitely, enabling police to retrospectively tail a suspect with remarkable precision.[6] And like CSLI, police need not identify the suspect in advance—Location History data is available for "numerous tens of millions" of Google users. *Chatrie*, 590 F. Supp. 3d at 907. Of course, a geofence limits the size and duration of any particular law enforcement data-grab. But *Carpenter*'s retrospectivity analysis emphasized the vast scope of *available* CSLI data, which gives police "*access* to a category of information otherwise unknowable." *Carpenter*, 585 U.S. at 312 (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 (quoting *Riley*, 573 U.S. at 403); *see United States v. Smith*, 110 F.4th 817, 836–38 (5th Cir. 2024). "The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). 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 (quoting *Jones*, 565 U.S. at 415 (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).

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

This case presents textbook examples of how police access to this digital information can invade the privacies of innocent users. At the suppression hearing,

---

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.

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

[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). 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).

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. 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 (1987) ("A search is a search, even if it happens to disclose nothing but the bottom of a turntable.").

Richardson Concurring Op., *infra*, at 81 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. 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 81. Respectfully, that is wrong on multiple accounts. Most obviously, it flat-out ignores the public surveillance doctrine. Tracking a person's "single, brief trip" on public thoroughfares (as in *Knotts*) is not a search; but tracking even an *object*'s trip in and out of a private space (as in *Karo*) *is* a search. *Compare Knotts*, 460 U.S. at 281 *with Karo*, 468 U.S. at 714–16. 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

[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.

records" puts them in a "qualitatively different category" from "telephone numbers and bank records." *Carpenter*, 585 U.S. at 309. *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. But *Carpenter* ultimately held that accessing the shorter span of data was enough to constitute a Fourth Amendment search. *Id*. at 310 n.3. 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 (citing *Jones*, 565 U.S. at 415 (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. 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. 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.

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. 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 (Sotomayor, J., concurring) (quoting *Lidster,* 540 U.S. at 426). 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 (Alito, J., concurring in the judgment).

Location History is like the GPS monitoring in *Jones*, only cheaper and more intrusive. Scholars have estimated that "tracking location by cell phone," as police did in *Carpenter*, "is almost twice as cheap as GPS tracking," which in turn is "twenty-eight times cheaper than covert pursuit." Ohm, *supra* n.4, at 369 (citing Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. Online 335, 354 (2014)). Location History tracking is likely even

cheaper. "With just the click of a button," Google—at the Government's request—"can access [its] deep repository of historical location information at practically no expense" to the Government. *Carpenter*, 585 U.S. at 311. And unlike the tracking device in *Jones*, which followed the suspect's Jeep on public roads, *see Jones* 565 U.S. at 403, Location History "follows its [subject] beyond public thoroughfares" and into private spaces, *Carpenter*, 585 U.S. at 311.

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. 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. 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. 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. 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

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

doctrine has been applied. *Carpenter*, 585 U.S. at 314. 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 (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. 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.

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. It can provide "not just dialed digits, but a detailed and comprehensive record of [a] person's movements." *Id.* at 309. And it is "effortlessly compiled," accessible at "the click of a button" and "at practically no expense." *Id.* at 309, 311.

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. 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. 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 (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 (quoting *Riley,* 573 U.S., at 385). 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.[12] Unlike the bank records and phone numbers in *Smith* and *Miller*, which were conveyed to companies by customers' physical, affirmative acts, the collection of CSLI is "inescapable and automatic," such that a cell phone user has "no way to avoid leaving behind a trail of location data." *Id.* at 315, 320.

Sharing Location History—while admittedly not wholly "inescapable"—is not meaningfully voluntary either. Most importantly, Location History is just one example of

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

a category of personal data–driven services that have become "indispensable to participation in modern society." *Id.* at 315. Nine in ten Americans own a smartphone,[13] and countless smartphone apps rely on users' personal data for both functionality and revenue. Consequently, Americans face enormous pressure to entrust detailed personal information to third parties in exchange for services. Tens of millions of citizens "opt" into services that collect and store years' worth of intimate information—including location history, medical records, financial data, family photos, private communications, and more—on remote servers managed by private corporations. Some of these services are simply convenient; others are mandated by employers; still others may be critical to a user's health or safety. Location History is a particularly useful and widely adopted example, used by "numerous tens of millions" for everyday services like traffic updates. *Chatrie*, 590 F. Supp. 3d at 907.

None of this means that Americans have ceded a reasonable expectation of privacy in their detailed private information. Smartphone users might reasonably expect that their deidentified data will be used, in aggregate, to fine-tune targeted advertising. But it would be a grave misjudgment to conflate an individual's limited disclosure to Google with an open invitation to the state. *See Jones*, 565 U.S. at 418 (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

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

protection."); *Smith*, 442 U.S. at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").

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

Approving a lucrative location-tracking feature on a smartphone is frictionless by design. Here, the record indicates that Location History can be enabled within a few moments of setting up and using an Android device like the one Chatrie used. One of the first steps in setting up a smartphone that runs on Android is to log into or create a Google account, a prerequisite for access to many of the smartphone's features, such as downloading apps, accessing Google Maps, or syncing Google services like Calendar and Contacts. The district court found that Google repeatedly prompts its millions of Android users to opt-in to Location History both upon initial set-up and then "multiple times across multiple apps." *Chatrie*, 590 F. Supp. 3d at 909; *see* J.A. 128–29.

As the district court recognized, Google's privacy warnings and descriptive pop-ups are "limited," "partially hidden," and "less than pellucid." *Chatrie*, 590 F. Supp. 3d at 936.

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

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

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

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.* (Sotomayor, J., concurring) ("[S]mart phone[] [owners] do not contemplate that these devices will be used to enable covert surveillance of their movements.").

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

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

In short, the single tap required to enable Location History does not represent a user's well-informed or meaningfully voluntary disclosure of "a comprehensive dossier of

his physical movements." *Carpenter*, 585 U.S. at 315. "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.'"

[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 81–83. 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 (noting that users "see a list of their long-distance (toll) calls on their monthly bills"). And in *Miller*, which was decided before the advent of online banking, the suspects physically brought the checks and deposit slips at issue to the bank. *Miller*, 425 U.S. at 442.

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. 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.

Carpenter, 585 U.S. at 314 (quoting *Riley*, 573 U.S. at 392). 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. The Government's acquisition of Chatrie's Location History "was a search within the meaning of the Fourth Amendment." *Id.* at 316.

IV.

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

Instead of addressing that compelling constitutional issue, this Court takes refuge in the good-faith exception—and thereby clears the path for widespread, surreptitious police surveillance. The result is plain. It leaves the door open for law enforcement to monitor religious services, political protests, gun shows, union meetings, or AA sessions—all without a warrant, all without judicial oversight or accountability. The technology at issue here does not merely capture a person's location at a single moment; it allows the Government to "reconstruct a person's movements." *Carpenter*, 585 U.S. at 312. 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 (Sotomayor, J., concurring) (citation omitted). A broad range of associational and expressive freedoms—private conversations, peaceful assembly, investigative journalism—can be chilled by the knowledge "that the Government may be watching." *Id.* "The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide." *Smith*, 442 U.S. at 751 (Marshall, J., dissenting).[16]

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

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

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

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

I. Background

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

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."

[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.

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

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

[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

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

---

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.

[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.

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

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

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

[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.

claims it saw a 1,500% increase in requests from 2017 to 2018 and a 500% increase from 2018 to 2019. Concerned with the potential threat to user privacy, Google consulted internal counsel and law enforcement agencies in 2018 and developed its own three-step procedure for responding to geofence requests. Since then, Google has objected to any geofence request that disregards this procedure.

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

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

[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.

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 (1984).

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

II. Discussion

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

The district court denied Chatrie's motion to suppress based on the good-faith exception. I agree that the motion should have been denied, but for an antecedent reason: Chatrie did not have a reasonable expectation of privacy in two hours' worth of Location History data voluntarily exposed to Google. So the government did not conduct a search when it obtained this information from Google, and so no warrant was required at all. The

district court should be affirmed on that straightforward basis. *See United States v. Smith*, 395 F.3d 516, 519 (4th Cir. 2005) (holding that we may affirm a district court "on any grounds apparent from the record").

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

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

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

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; *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 (1967). Under *Katz*, a search occurs when the government invades an individual's reasonable expectation of privacy. *Id.* at 351; *id.* at 360 (Harlan, J., concurring); *see also Smith v. Maryland*, 442 U.S. 735, 740 (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; *Carpenter*, 585 U.S. at 304.

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. 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 (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.* in 443. 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.[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

[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 (1971), and tax documents given to an accountant, *Couch v. United States*, 409 U.S. 322, 335 (1973).

third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). If they lack Fourth Amendment protections for any electronically shared data, then the government could access whole swaths of private information free from constitutional scrutiny.

The Supreme Court addressed this tension in a series of cases involving the government's use of location-tracking technology. First, in *United States v. Knotts*, the Court held that the government did not conduct a search when it placed a tracking device in a container purchased by one of Knotts's coconspirators and used it to monitor his short trip to Knott's cabin. 460 U.S. 276, 278–80 (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. 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. Yet the Court reserved whether it would treat long-term surveillance differently. *Id.* at 283–84.[11]

[11] Separately, the Court held that police did not conduct a search when they observed the beeper on the premises of Knotts's cabin. *Knotts*, 460 U.S. at 284–85. "[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. 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 (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. The Court held

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. 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. 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 (Alito, J., concurring in the judgment); *id.* at 415 (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 (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

---

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. 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. It therefore intruded on the reasonable expectation of privacy of all who had a Fourth Amendment interest in that home. *Id.* at 719 (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 (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 (distinguishing *Rawlings v. Kentucky*, 448 U.S. 98 (1980), since the defendant in that case did not have a reasonable expectation of privacy in the place searched).

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. 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.[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. 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. 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. The Court thus explained that CSLI provides law enforcement "an all-encompassing record of the holder's whereabouts" over that period, *id.* at 311, 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 (2014); and then quoting *Jones*, 565 U.S. at 415 (opinion of Sotomayor, J.)). Such access—at least, to seven

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

days' worth of CSLI—invades the reasonable expectation of privacy individuals have "in the whole of their physical movements." *Id.* at 310 & n.3.

That Carpenter "shared" his CSLI with his wireless carriers didn't change the Court's conclusion. *Id*. at 314. 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). 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 (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.

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). 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). 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. 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.

Three years later, we clarified the scope of *Carpenter*'s holding in *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021) (en banc). *Beautiful Struggle* involved a Fourth Amendment challenge to the City of Baltimore's aerial-surveillance program. *Id*. at 333. The program captured aerial photos of thirty-two square city miles every second for "at least 40 hours a week, obtaining an estimated twelve hours of coverage of around 90% of the city each day." *Id.* at 334. We interpreted *Carpenter* to "solidif[y] the line between short-term tracking of public movements—akin to what law enforcement could do '[p]rior to the digital age'—and prolonged tracking that can reveal intimate details through habits and patterns." *Id.* at 341 (second alteration in original) (quoting *Carpenter*, 585 U.S. at 310). 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). 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 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

[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).

[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 (holding that the third-party doctrine did not apply to the involuntary disclosure of expansive data).

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. 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. All the government had was an "individual trip viewed in isolation," which, standing alone, was not enough to "enable[] deductions about 'what [Chatrie] does

[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) (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").

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 (quoting *Knotts*, 460 U.S. at 281).[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; *Smith*, 442 U.S. at 742. 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 (quoting *Miller*, 425 U.S. at 442).

Furthermore, Chatrie voluntarily exposed his location information to Google by opting in to Location History. *Id.* at 315. Consider again how Location History works.

---

[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; *Kyllo*, 533 U.S. at 40. 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 (1978); *Brown v. United States*, 411 U.S. 223, 230 (1973).

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

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 (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

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

life' that [activating it] is indispensable to participation in modern society." *Carpenter*, 585 U.S. at 315 (quoting *Riley*, 573 U.S. at 385). *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 (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. 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). 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. He cannot now claim to have had a reasonable expectation of privacy in this information. *See Smith*, 442 U.S. at 743–44. 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

[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 (Kennedy, J., dissenting); *id.* at 353–54 (Thomas, J., dissenting); *id.* at 402 (Gorsuch, J., dissenting). Nor does he claim that he could bring a tort suit if this information were stolen. *See id.* at 353 (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.

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 district court rightly declined to prescribe the "strong medicine" of excluding otherwise admissible evidence. *United States v. Janis*, 428 U.S. 433, 453 (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 (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 (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 (1974) (first quote); *Davis*, 564 U.S. at 236–37 (second quote).

"Real deterrent value is a necessary condition for exclusion, but it is not a sufficient one." *Davis*, 564 U.S. at 237 (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. In contrast, when law enforcement officials "act with an objectively reasonable good-faith belief that their conduct is lawful," "the deterrence

rationale loses much of its force, and exclusion cannot pay its way." *Davis*, 564 U.S. at 238 (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 (quotation marks removed). But here there were no clear guideposts to follow. The investigating officer was using "rapidly developing technology" while faced with a "dearth of court precedent." *United States v. McLamb*, 880 F.3d 685, 691 (4th Cir. 2018) (first quote); *United States v. Smith*, 110 F.4th 817, 840 (5th Cir. 2024) (second quote). Indeed, when the officer was investigating this case, it appears no court had examined the validity of (or constitutional restrictions on) geofence warrants.

Second, the officer did what we expect reasonable officers to do when faced with such uncertainty. The officer knew he "had sought three other geofence warrants in the past" that magistrates had approved. JA 1349; see *United States v. Carpenter*, 926 F.3d 313, 318 (6th Cir. 2019) (noting that, at the relevant time, "[t]wo magistrate judges" had issued orders based on the same statute the Supreme Court later held could not constitutionally justify obtaining the defendant's cell-site location information without a warrant). "Before seeking those warrants," the officer "consulted with prosecutors, who approved them." JA 1349; see *McLamb*, 880 F.3d at 691 (noting officers had "consulted with attorneys from the Department of Justice"); *Smith*, 110 F.4th at 839 (officers "had conversations with other law enforcement officers and the U.S. Attorney's Office prior to

submitting their warrant"). And here, for the fourth time, the officer sought and obtained a warrant from a judicial officer.

The Supreme Court has said the exclusionary rule should be used to "deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring*, 555 U.S. at 144. 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 (quotation marks removed).

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

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

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

In its first request, the Government asked Google to produce a dataset showing pseudonymized[1] Google users' movements within a 150-meter radius of the bank—the initial "geofence"—during the one-hour period surrounding the robbery. Because of 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.

narrow parameters of this request, the pseudonymized Location History was not likely to be traceable to the identities of particular Google users.

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

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

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

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 (2018), however, I would hold that individuals do have a reasonable expectation of privacy in their *non-anonymous* Location History data. This includes pseudonymized data that, based on the parameters of a particular request, is likely to be traceable to the identities of specific individuals. The Government thus conducted a Fourth Amendment search when it acquired Chatrie's non-anonymous Location History data through its second and third requests to Google.

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

I. **Background**

On the afternoon of May 20, 2019, an unknown individual robbed a bank in Virginia. The robber pointed a gun at the bank manager and stole approximately $195,000.

He then fled the scene before police could respond, and law enforcement was unable to find him through witness accounts, tips, and security footage.

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

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

Location History logs comprehensive and precise data from cellphones that enable location tracking. Location History records a phone's location approximately every two minutes. In certain circumstances, Google can estimate a phone's location down to three meters. Location History even allows Google to estimate a phone's elevation, with

precision that can potentially infer the specific floor of an apartment building where a user is located. To show a phone's location, Location History displays a point on a map and depicts around that point a radius known as a "confidence interval." The smaller the radius around a phone's estimated location, the more confident Google is in that phone's exact location. A phone is somewhere inside the given confidence interval over two-thirds of the time.

Several years ago, Google worked with law enforcement to develop a three-step process for responding to geofence warrants. Each "step" begins with a new request from law enforcement to Google. The Government in this case followed Google's three-step process. It is worth emphasizing that Google's three-step process was neither designed nor mandated by a magistrate. The process merely expresses the preferences and policy of Google, a private company.

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

At step one, the Government requested pseudonymized data showing all Google users' movements within a 150-meter radius of the bank during the one-hour period surrounding the robbery. The geofence perimeter primarily encompassed public streets. In response to the Government's first request, Google produced a pseudonymized dataset that

consisted of 210 discrete location datapoints across 19 unique phones, meaning that the Government obtained numerous datapoints from some of those phones.

After reviewing the data that Google provided in response to the first request, the Government next requested from Google additional Location History data on some of the users identified within the initial geofence. In its second request, the Government asked Google to produce two hours of full Location History data—both inside and outside of the 150-meter geofence—generated by nine of the 19 Google users identified pseudonymously at step one.

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

II. Analysis

A. The Third-Party Doctrine and *Carpenter*

The government conducts a Fourth Amendment search when it invades an individual's "reasonable" expectation of privacy. *See Katz v. United States*, 389 U.S. 347, 360–62 (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 (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. Chatrie argues that the Government violated his Fourth Amendment rights when it obtained his Location History data without a valid warrant. Chatrie cannot rely on the Fourth Amendment's protections unless he held a reasonable expectation of privacy in that Location History data.[2]

The *Katz* test applies to all searches and seizures. For a subset of cases within this Fourth Amendment framework, however, additional principles guide courts in evaluating whether an expectation of privacy is "reasonable." "No single rubric definitively resolves which expectations of privacy" are reasonable. *Carpenter*, 585 U.S. at 304. "[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 (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 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), drew "a line between what a person keeps to himself and what he shares with others." *Carpenter*, 585 U.S. at 307–08. In describing *Miller* and *Smith*, the *Carpenter*

[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 (2018).

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 (quoting *Smith*, 442 U.S. at 743–44 (first quote); *Miller*, 425 U.S. at 443 (second quote) (internal citations omitted)). Under this doctrine, "the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections." *Id.*

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

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. 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. 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.

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. 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 301–02. It requested from telecommunications carriers a form of data known as cell-site location information (CSLI). *Id.* at 301. 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. 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.

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. 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. 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. 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. 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.

The *Carpenter* Court rejected the government's invocation of the third-party doctrine. It stated that "there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller*," the cases that form the core of the third-party

doctrine, "and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id.* at 314. 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. 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.

B. *Carpenter*'s Application to this Case

Applying *Carpenter*'s two factors to this case, I would hold that law enforcement conducts a search when it obtains any amount of an individual's Location History data that is non-anonymous. This includes Chatrie's Location History data that the Government

obtained through its second and third[3] requests to Google. These requests sought highly revealing data, and the record does not establish whether the disclosure of this information was definitively voluntary.

i. *Non-Anonymous Location History Data is Highly Revealing*

The Government contends that because Chatrie's disclosure of his Location History data to Google was voluntary, he forfeited any expectation of privacy in that data. Yet

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

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

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

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 (emphasis added). *Carpenter* described "voluntary exposure" as the "second rationale underlying the third-party doctrine." *Id.* at 315. 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.

Pseudonymized location data is not anonymous when it can be linked to a particular individual. Whether pseudonymized Location History data is likely to be traceable to a specific person—an inquiry that must be conducted at the time of a request, not *post-hoc*—depends on (1) the duration of the request; (2) the size of the search area; and (3) the nature of the search area. The second and third factors are particularly important. Let's take an example. If the government were to look at pseudonymized Location History data generated within a defined section of I-95 between 7:00 am and 9:00 am on a weekday, it is not likely to be able to determine the identities of the individual drivers. If, on the other

hand, the search area were unrestricted or included residential neighborhoods, two hours of Location History data during that same time period could reveal that a pseudonymized Google user traveled from a particular home to a particular company's office building. The government could readily determine that individual user's identity by, for instance, looking at property records and running a LinkedIn search.

This court's en banc decision in *Leaders of a Beautiful Struggle v. Baltimore Police Department* recognized that location data without individual identifiers can still pose a threat to privacy. 2 F.4th 330, 341–42 (4th Cir. 2021). In that case, the government contended that an aerial surveillance program did not infringe upon individuals' reasonable expectations of privacy because it showed people only as "a series of anonymous dots traversing a map of Baltimore." *Id.* at 342 (quotation omitted). This court emphasized, however, that the particular movements of these dots, "analyzed with other available information, will often be enough for law enforcement to deduce the people behind the pixels." *Id.* at 343.

The pseudonymized Location History data obtained through the Government's first request was anonymous. In that request, the Government sought data depicting all Google users' movements within a 150-meter radius, which encompassed primarily public streets and stores, over a one-hour timeframe. Absent some stroke of luck for the Government, it was exceedingly unlikely that Google's response would reveal the identities of the pseudonymized individuals within that geofence perimeter, even if "analyzed with other available information." *Id.* Through its second request to Google, however, the Government obtained two hours of Location History data belonging to nine

pseudonymized individuals. That Location History data was not confined to any geographic boundary. At the time of the second request, law enforcement could have predicted that the pseudonymized data would likely be traceable to Chatrie and the other Google users. As a result, it was non-anonymous.

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

[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 (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.

recognize that CSLI is an entirely different *species* of business record." *Id.* at 318 (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. Whereas past "attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection," Location History data allows the government to "travel back in time to retrace a person's

whereabouts, subject only to the retention polices of the wireless carriers." *Id.* Google retains Location History data indefinitely—even longer than the five-year period that the carriers at issue in *Carpenter* maintained CSLI. *See id.*

Also like CSLI, Location History data can detail a log of a person's movements over several years. Critically, however, non-anonymous Location History data is far more revealing than CSLI. Judge Wynn pointedly explains the differences. *See* opinion of WYNN, J., at 45-46. Location History has the capacity to record a user's location every two minutes, or an average of 720 times per day. CSLI, in contrast, logged Carpenter's location an average of 101 times per day. *Carpenter*, 585 U.S. at 302. Location History data is thus more "detailed" and "encyclopedic" than CSLI. *Id.* at 309. 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, Location History can pinpoint an individual's location within three meters. Because non-anonymous Location History data is highly revealing, the first *Carpenter* factor weighs in favor of Chatrie.

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

Carpenter requires us to balance the revealing nature of non-anonymous Location History data against a second consideration, the voluntariness with which it is disclosed to Google. Whether the disclosure of data to a third party was "voluntary" is not a binary inquiry but a matter of degree. Here, this factor does not tip decisively in favor of either party. Though the Government describes Location History as a voluntary feature that a user must "affirmatively enable," J.A. 1337, the record shows that individuals may enable

Location History without meaningfully consenting to data collection, or at least without understanding the implications of the feature.

Google claims that Location History is disabled by default. Yet for those who download certain Google apps—including popular apps such as Google Maps, Google Photos, and Google Assistant—there is no "default" setting. Google repeatedly requires users to make a choice. Through pop-up permission screens, users are asked either to grant or deny Google permission to track their location.

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

Google stated that approximately two-thirds of its "active users" have declined to enable Location History, but this figure is misleading. One of Google's experts testified that "active Google users" includes anyone with a Google account on any device, including a computer. That would include those who never downloaded a Google app and were thus never presented with the choice of enabling Location History. Google does not claim that two-thirds of its users, when confronted with a pop-up permission screen, selected "NO THANKS" rather than "TURN ON." Indeed, Google has provided no data about the percentage of users who declined to enable Location History when prompted to do so. Further, the fact that most Google users' settings were different than Chatrie's does not suggest that he intentionally selected his particular settings, or that they intentionally selected theirs.

Even after reviewing all available information about Location History provided by Google, a user would struggle to determine where his Location History data is stored. Google does not explicitly inform users whether Location History data is stored locally on each phone, or whether it is stored on Google's servers and accessible to Google employees. Further, Google's warnings do not indicate how many times a day Location History data will be collected. The third-party doctrine concerns data that one "knowingly share[s]" with a third party. *Carpenter*, 585 U.S. at 298. 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 (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 (1979). The

government cannot, for example, search every unit in an apartment building because it has probable cause to believe that some unknown part of the building holds evidence of a crime. *See* Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 4.5(b) (6th ed. 2024); *United States v. Clark*, 638 F.3d 89, 95 (2d Cir. 2011); *cf. Maryland v. Garrison*, 480 U.S. 79, 88 n.13 (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 (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. Those stops—executed without individualized suspicion—were constitutional only because they were conducted to identify witnesses, not suspects. *Id.* at 423. 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. 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. In contrast, *Indianapolis v. Edmond*, 531 U.S. 32 (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.

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

The Government's reliance on *Zurcher v. Stanford Daily* is similarly misplaced. 436 U.S. 547 (1978). In *Stanford Daily*, as in this case, the government applied for a search warrant without particular suspects in mind. *Id.* at 550–51. 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. 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. As a result, the government had probable cause to conduct the *only* search at issue: the search of the Stanford Daily's office.

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

Analyzing Google's anonymous data may have given the Government probable cause subsequently to obtain a warrant for non-anonymous data. Had the detective gone to a magistrate after analyzing the Google data he received in response to the first request, he may have been able to articulate probable cause to search the Location History of particular Google users, including Chatrie. The detective never went back to the magistrate, however. He sought judicial authorization only once—prior to the first request to Google. Because the detective could not explain why he would eventually search the Location History data of certain, then-unknown users in Google's dataset, he failed to show probable cause to conduct the second and third requests. Under the terms of the geofence warrant, Google, not a magistrate, was the sole entity that could confine the scope of the ultimate search. Probable cause determinations cannot be delegated to private entities. *Cf. Birchfield v.*

North Dakota, 579 U.S. 438, 469 (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)). The proper focus of our inquiry is the data the government obtains, not the size of Google's database. Though the Fifth Circuit refers to this proposition as "breathtaking," *Smith*, 110 F.4th at 838 n.12, any other approach would be nonsensical. The scope of a search does not depend on what a company's compliance officer incidentally encounters—but never discloses to law enforcement—while looking through the company's database to fulfill a particular request. In *Carpenter*, for example, the duration of the search would not have changed had Sprint stored the requested CSLI in a spreadsheet that contained additional days of CSLI data. Because the detective's first request did not amount to a search of any individual in Google's database, the Fourth Amendment did not require the detective to establish probable cause before submitting that request.[5]

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

[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.

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 (2018) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)), and requires that law enforcement obtain a warrant prior to conducting a search, *id.* at 304 (citing *Smith v. Maryland*, 442 U.S. 735, 740 (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 (2011), and only applies where its application will "deter future Fourth Amendment violations," *id*. at 236–37; *see also Stephens*, 764 F.3d at 335; *Illinois v. Krull*, 480 U.S. 340, 347 (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 (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 (2009) (internal quotation marks omitted).

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

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

I.

Google account users can opt in to location history on their mobile devices, which allows users to keep track of locations they have visited. J.A. 127. At the time of the offense, Google processed and stored this location history if users shared it via location reporting. J.A. 125, 129–30. Pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, law enforcement can obtain legal process compelling Google to disclose location information, including through geofence warrants. J.A. 124–25. In conjunction with the Department of Justice, Google developed a three-step anonymization and narrowing protocol in response to these geofence requests. J.A. 1344.

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

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

[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).

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. 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 (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. 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. 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. 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.

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

Additionally, Detective Hylton had unbridled discretion to determine who would be subject to intrusive and expansive searches. For example, at Step Two, Detective Hylton initially requested additional location data for all nineteen users identified at Step One, expanded for thirty minutes before and thirty minutes after the originally requested one hour window, and without any geographic limitations. J.A. 1354–55; *see also* J.A. 98. His email to Google stated that he was requesting the additional data "in an effort to rule out

possible co-conspirators," and that nine of the users "may fit the more likely profile of parties involved." J.A. 98. At oral argument, the government contended that it was looking for witnesses as well. *See* Oral Argument at 53:51. Detective Hylton followed up on his email twice on the two following days. J.A. 100, 1059. He then left two voicemails for a Google specialist; the specialist returned his call and recounted the issues in Detective Hylton's email, describing how his request did not follow the three-step process and explaining the importance of narrowing his request. J.A. 102, 1584–85. The next day, Detective Hylton sent an email narrowing his request to nine users. J.A. 102, 1059, 1584. Google provided Detective Hylton the anonymized, expanded data for nine users. J.A. 1585. As was explained before, the government cannot explain how or why Detective Hylton narrowed in on the particular users. And at no point during this process did Detective Hylton seek judicial intervention, although the warrant did not contain sufficient probable cause and particularity to authorize these additional searches.

Detective Hylton could not have reasonably believed that the liberty authorized by the warrant was constitutional given the lack of specificity the Fourth Amendment explicitly demands.[2] *United States v. Groh*, 540 U.S. 551, 563 (2004) (citing *Harlow v. Fitzgerald*, 457 U.S. 800, 818–19 (1982)) ("Given that the particularity requirement is set forth in the test of the Constitution, no reasonable officer could believe that a warrant that

[2] *See, e.g.*, *Groh v. Ramirez*, 540 U.S. 551 (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).

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 indiscretions. Exclusion of the evidence is therefore appropriate here.

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

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

Amendment violations. Indeed, the Supreme Court has said as much. Specifically, the Supreme Court stated "that [t]he efforts of the courts and their officials to bring the guilty to punishment, praiseworthy as they are, are not to be aided by the sacrifice of those great [constitutional] principles." *Mapp v. Ohio*, 367 U.S. 643, 648 (1961) (quoting *Weeks v. United States*, 232 U.S. 383, 391–92 (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 (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 (citing *U.S. v. Johnson*, 457 U.S. 537, 561 (1982)) (internal quotation marks omitted). If we permitted that course of action, Fourth Amendment protections would become a nullity in the face of rapidly emerging technology.

The same unfortunate fate would result if Detective Hylton's belief in his actions was dispositive. *Leon* instructs us to assess whether the investigating officer held an objectively reasonable belief in the warrant's validity and his actions. 468 U.S. at 919. 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) (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 ("Good faith on the part of the arresting officers is not enough") (citing *Henry v. United States*, 361 U.S. 98, 102 (1959)) (internal brackets and quotation marks omitted). If subjective good faith alone were the test, the protections of the Fourth Amendment would evaporate, and the people would be "'secure in their persons, houses, papers, and effects,' only in the discretion of the police." *Id*.

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

II.

Law enforcement should not be denied the benefit of the efficiencies that emerging technologies offer. However, when seeking digital evidence, officers must demonstrate at least the same level of supporting information necessary to justify the search of physical places and things. In other words, officers should not be permitted, with aid of an unbridled warrant, to shake the proverbial digital tree without an objectively reasonable belief that the warrant and the manner of its execution are consistent with the Fourth Amendment. And that reasonable belief must be founded on something more than the commonality of

the technology at issue in the case. This is especially so given that technology has and continues to shift our understanding of "person, place, or thing."

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

The Constitution nor Fourth Amendment precedent to date anticipated that person may one day refer to a non-human, such as Optimus; places could encompass locations in the Metaverse (or otherwise only digitally accessible); and things could include intangible objects that exist only electronically. Given that reality, the judiciary still must fulfill its role and duty to ensure that the interpretation of the Constitution does not fall solely in the hands of anyone not charged with protecting the rights it guarantees. Our Court failed to do so here. Thus, I must dissent.