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.

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: December 8, 2023 Decided: July 9, 2024

Before WILKINSON, WYNN, and RICHARDSON, Circuit Judges.

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

ARGUED: Michael William Price, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, Washington, D.C., for Appellant. Nathan Paul Judish, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellee. **ON BRIEF:** Geremy C. Kamens, Federal Public Defender, Alexandria, Virginia, Laura J. Koenig, Assistant Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Richmond, Virginia, for Appellant. Kenneth A. Polite, Jr., Assistant Attorney General, Richard W. Downing, Deputy Assistant Attorney General, Computer Crime and Intellectual Property Section, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C.; Jessica D. Aber, United States Attorney, Kenneth R. Simon, Jr., Assistant United States Attorney, Peter S. Duffey, Assistant United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Richmond, Virginia, for Appellee. Jennifer Lynch, Andrew Crocker, Hannah Zhao, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California; Jacob M. Karr, Technology Law and Policy Clinic, NEW YORK UNIVERSITY SCHOOL OF LAW, New York, New York, for Amici Technology Law and Policy Clinic at New York University School of Law and Electronic Frontier Foundation. Jennifer Stisa Granick, San Francisco, California, Nathan Freed Wessler, Ashley Gorski, Patrick Toomey, Brandon Buskey, Trisha Trigilio, Laura Moraff, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York; Eden B. Heilman, Matthew W. Callahan, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA, Richmond, Virginia; William F. Nettles, IV, Federal Public Defender, Columbia, South Carolina, G. Alan DuBois, Federal Public Defender, Raleigh, North Carolina, Louis Allen, Federal Public Defender, Greensboro, North Carolina, Juval O. Scott, Federal Public Defender, Roanoke, Virginia, Brian J. Kornbrath, Federal Public Defender, Clarksburg, West Virginia, James Wyda, Federal Public Defender, Baltimore, Maryland, Wesley P. Page, Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Charleston, West Virginia; John Baker, Federal Public Defender, FEDERAL DEFENDERS OF WESTERN NORTH CAROLINA, INC., Charlotte, North Carolina, for Amici American Civil Liberties Union, American Civil Liberties Union of Virginia, and Eight Federal Public Defender Offices Within the Fourth Circuit. Bruce D. Brown, Katie Townsend, Gabe Rottman, Grayson Clary, Emily Hockett, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, Washington, D.C., for Amicus Reporters Committee for Freedom of the Press.

RICHARDSON, Circuit Judge:

Okello Chatrie appeals the district court's denial of his motion to suppress location data obtained using a geofence warrant. He argues that the geofence warrant violated the Fourth Amendment because it lacked probable cause and particularity. But we find that the government did not conduct a Fourth Amendment search when it obtained two hours' worth of Chatrie's location information, since he voluntarily exposed this information to Google. We therefore affirm the district court.

I. Background

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

A. Google Location History and Geofence Warrants

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

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

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 (Continued)

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 in

[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.

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

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

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

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

The district court denied Chatrie's motion to suppress based on the good-faith exception. We agree that the motion should be denied, but for a different reason: Chatrie did not have a reasonable expectation of privacy in two hours' worth of Location History data voluntarily exposed to Google. So the government did not conduct a search when it obtained this information from Google. We therefore affirm the district court's decision.

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

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

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. To trigger its protections, the government must conduct a "search" (or "seizure") covered by the Fourth Amendment. "For much of our history, Fourth Amendment search doctrine was 'tied to common-law trespass' and focused on whether the government 'obtains information by physically intruding on a constitutionally protected area.'" *Carpenter v. United States*, 585 U.S. 296, 304 (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. 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 *United States v. Miller*, the Court held that the government did not conduct a search when it obtained an individual's bank records from his bank, since he voluntarily exposed those records to the bank in the ordinary course of business. *Id.* in 443. Likewise, in *Smith v. Maryland*, the Court held that the government did not conduct a search when it used a pen register to record outgoing phone numbers dialed from a person's telephone, because he voluntarily conveyed those numbers to his phone company when placing calls. 442 U.S. at 742.[10]

Despite its clear mandate, the third-party doctrine has proved difficult to implement in the digital age. After all, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). If they lack Fourth Amendment protections for any

[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).

electronically shared data, then the government could access whole swaths of private information free from constitutional scrutiny.

The Court addressed this tension in a series of cases involving the government's use of location-tracking technology. First, in *United States v. Knotts*, the Court held that the government did not conduct a search when it placed a tracking device in a container purchased by one of Knotts's co-conspirators and used it to monitor his short trip to Knott's cabin. 460 U.S. 276, 278–80 (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 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 (Continued)

This issue later resurfaced in *United States v. Jones*, 565 U.S. 400. There, the government attached a GPS device to Jones's automobile and used it to track his movements for twenty-eight days. *Id.* at 402–04. 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 *Carpenter v. United States*, 585 U.S. 296. *Carpenter* involved government access to

---

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).

historical cell-site location information ("CSLI")—a time-stamped record that is automatically generated every time any cell phone connects to a cell site. *Id.* at 300–01. 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 a warrant. *Id.*

The Court began by noting that government access to CSLI "does not fit neatly under existing precedents" but "lie[s] at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake." *Id.* at 306. Starting with the location-tracking cases, the Court found that CSLI "partakes of many of the qualities"—and in some ways, exceeds them—"of the GPS monitoring we considered in *Jones*." *Id.* at 309–13. 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—

[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.

at least, to 7 days' worth of CSLI—invades the reasonable expectation of privacy individuals have "in the whole of their physical movements." *Id.* at 310 & n.3.

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 CSLI. *Id.* It first considered "'the nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'" *Id.* (quoting *Miller*, 425 U.S. at 442). 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 this 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 7 days' worth of historical CSLI is a search within the meaning of the Fourth Amendment. *Id.* at 316, 310 n.3.[13]

Three years later, we clarified the scope of *Carpenter*'s holding in *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021) (en banc). *Beautiful Struggle* involved a Fourth Amendment challenge to the City of Baltimore's aerial-surveillance program. *Id*. at 333. The program captured aerial photos of thirty-two square city miles every second for "at least 40 hours a week, obtaining an estimated twelve hours of coverage of around 90% of the city each day." *Id.* at 334. We interpreted *Carpenter* to "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)

[13] The dissent reads *Carpenter* to hold that access to just 2 days' worth of CSLI is a search. Diss. Op. at 65. But even though one of the wireless carriers produced only 2 days' worth of CSLI in response to the government's request for 7 days' worth, *Carpenter* only held that "accessing *seven days* of CSLI constitutes a Fourth Amendment search." *Carpenter*, 585 U.S. at 310 n.3 (emphasis added).

(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.[14]

B. Application

Relying on *Carpenter*, Chatrie argues that the government conducted a search when it obtained his Location History data from Google.[15] We disagree. *Carpenter* identified two rationales that justify applying the third-party doctrine: the limited degree to which the information sought implicates privacy concerns and the voluntary exposure of that information to third parties. Both rationales apply here. Accordingly, we find that Chatrie

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

[15] Chatrie does not argue that the government conducted a search when it obtained his subscriber information from Google at Step Three of the geofence warrant process. This is probably because we have already held that individuals do not have a reasonable expectation of privacy in subscriber information they provide to an internet provider. *See United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010). Chatrie does not ask us to revisit this holding in light of *Carpenter*, so here we consider only whether the government's access of his Location History data was a search.

did not have a reasonable expectation of privacy in the two hours' worth of Location History data that law enforcement obtained from Google. So the government did not conduct a search by obtaining it.

Start with the nature of the information sought. *Carpenter*, 585 U.S. at 314. The government requested and obtained only two hours' worth of Chatrie's Location History data.[16] By no means was this an "all-encompassing record of [Chatrie's] whereabouts . . . provid[ing] an intimate window into [his] person[al] life." *Carpenter*, 585 U.S. at 311. All the government had was an "individual trip viewed in isolation," which, standing alone, was not enough to "enable[] deductions about 'what [Chatrie] does repeatedly, what he does not do, and what he does ensemble.'"[17] *Beautiful Struggle*, 2 F.4th at 342 (quoting *Maynard*, 615 F.3d at 562–63). The information obtained was therefore far less revealing

[16] At argument, Chatrie suggested that the search occurred when *Google* looked through its entire Location History database at the government's behest. But *Carpenter* and *Beautiful Struggle* both held that a search only occurs once the *government* accesses the requested information. *See Beautiful Struggle*, 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)). So the proper focus of our inquiry is whether the government's access to two hours' worth of Chatrie's Location History data was a search.

[17] Chatrie raises the possibility that a geofence warrant could reveal a person's movements within a constitutionally protected space, like his home. *See Karo*, 468 U.S. at 716–17; *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).

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).[18] A record of a person's single, brief trip is no more revealing than his bank records or telephone call logs. *See Miller*, 425 U.S. at 442; *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. 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

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

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.[19] A user cannot opt in to Location History without seeing this text.

So unlike with CSLI, a user knowingly and voluntarily exposes his Location History data to Google. First, Location History is not "'such a pervasive and insistent part of daily life' that [activating it] is indispensable to participation in modern society." *Carpenter*, 585 U.S. at 315 (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.

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

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.[20]

C. Responding to the Dissent

In our view, this case involves a straightforward application of the third-party doctrine. But the dissent disagrees. Unlike us, the dissent reads *Carpenter* to have abandoned both strands of doctrine that preceded it, at least when the government uses new technology to monitor a person's movements. In their place, the dissent explains, the Court

---

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

Even if we found that Chatrie did not forfeit this issue, we would still reject it on the merits. Chatrie does not cite any positive law (state or federal) that gives him an ownership interest in his Location History data. *See Carpenter*, 585 U.S. at 331 (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.

concocted anew a four (or five?) factor balancing test that considers whether police obtained information that was comprehensive, retrospective, intimate, easy to access, and (perhaps?) voluntarily exposed. Diss. Op. at 49–51. The dissent then puts a pot on the fire, combines these ingredients, and *voila!*—finds that the police conducted a search here.

For all its bold pronouncements, the dissent's novel framework only works if you interpret *Carpenter* to have jettisoned both lines of cases that preceded it and created a new inquiry from scratch. Indeed, this thesis seems to undergird the dissent's entire argument, as it repeats it over and over.[21] Contrary to the dissent's claims, however, *Carpenter* did not cast away the decisions that preceded it. Rather, the Court explicitly stated that both the *Knotts-Jones* and the *Smith-Miller* lines of cases "inform our understanding of the privacy interests at stake." 585 U.S. at 306. It then went on to apply the principles announced in the location-tracking cases, *id*. at 310, and to distinguish—based on the unique features of CSLI—the third-party cases, *id*. at 313–16.

[21] *See, e.g.*, Diss. Op. at 47 ("Both lines of cases would seemingly 'inform our understanding of the privacy interests at stake,' . . . but neither squarely applies because this kind of data constitutes a 'qualitatively different category' of information . . . ." (first quoting *Carpenter*, 585 U.S. at 306; then quoting *id.* at 309)); *id.* at 48 ("After concluding that no existing Fourth Amendment doctrine applied neatly to such a digital innovation, the *Carpenter* Court applied a new framework based on the historical understandings of privacy protections that it had described and concluded that the CSLI obtained 'was the product of a search' that required a warrant." (quoting *Carpenter*, 585 U.S. at 310)); *id.* at 51 ("Put simply, the Court declined to extend existing doctrines to exempt CSLI from Fourth Amendment protections based on the principle that it first recognized decades earlier: previously unimaginable technology that reveals unprecedented amounts of personal information requires new rules."); *id.* at 52 ("To sum up, the Court concluded that 'personal location information maintained by a third party' lies at the intersection of the public-surveillance and third-party cases, but that neither theory 'neatly' applies." (quoting *Carpenter*, 585 U.S. at 306)).

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

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

But you don't have to take our word for it. Rather look to our en banc opinion in *Beautiful Struggle*. 2 F.4th 330. *Beautiful Struggle* was our first application of *Carpenter* to novel location-tracking technology. Yet nowhere in that opinion did we suggest that

Carpenter departed from cases like *Knotts* and *Jones* and created a new, factor-based inquiry. On the contrary, we recognized that "[t]he touchstone in *Carpenter* was the line of cases addressing 'a person's expectation of privacy in [their] physical location and movements,'" *i.e.*, *Knotts* and *Jones*. 2 F.4th at 340 (alteration in original) (quoting *Carpenter*, 585 U.S. at 306–07)). We then explained that

> *Carpenter* solidified the line between short-term tracking of public movements—akin to what law enforcement could do '[p]rior to the digital age'—and prolonged tracking that can reveal intimate details through habits and patterns. . . . The latter form of surveillance invades the reasonable expectation of privacy that individuals have in the whole of their movements and therefore requires a warrant.

Id. at 341 (alteration in original). Far from recognizing any sort of factor-based inquiry, therefore, *Beautiful Struggle* announced the exact line we draw here—that police invade an individual's reasonable expectation of privacy in the whole of his physical movements when they use technology to monitor his long-term movements, but not when they glimpse only his short-term movements. *See also id.* at 345 ("People understand that they may be filmed by security cameras on city streets, or a police officer could stake out their house and tail them for a time. . . . But capturing everyone's movements outside during the daytime for 45 days goes beyond that ordinary capacity.").

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

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

---

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

> The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more. . . . Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit,

(Continued)

The dissent misses *Beautiful Struggle*'s distinction when it catalogues the kind of private details that could be learned from two hours' worth of Location History. According to the dissent, a two-hour snippet of Location History could reveal a wealth of otherwise unknowable and intimate information, like a person's "romantic rendezvous," "medical appointments," or "afternoon and early-evening routines." Diss. Op. at 63. But the theory adopted in *Beautiful Struggle* rejects this exact proposition. To be sure, a two-hour snippet might show that someone visited an apartment, swung by a doctor's office, and then popped into a gym. Yet glimpsing this single trip in isolation could not itself enable sound deductions about that person's habits, routines, and associations. For example, he may have visited the apartment because he is having an affair, but he equally could have been seeing a friend for coffee, touring a housing upgrade, or buying a couch off of Facebook marketplace. Similarly, he might have visited the doctor's office for his appointment, yet he also could have been dropping off his spouse or collecting information about the doctor's services or needs. And observing someone enter a gym once certainly cannot confirm whether he is a gym rat or simply riding a New Years high. Only by observing

---

> as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.

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

that person's movements over a longer period could the police reliably deduce his habits, routines, and associations. No such deductions could accurately be made from a mere two-hour glimpse.[23]

Applying this theory here leads to a straightforward conclusion. As the dissent correctly observes, Location History has capabilities much like GPS data and CSLI. But unlike in *Carpenter* or *Jones*, the government in this case obtained only two hours' worth of Chatrie's Location History data. Although this brief glimpse into his whereabouts may have revealed the locations he visited, it was plainly insufficient to offer insight into his habits, routines, and associations. So the government did not invade his "legitimate 'expectation of privacy'" by obtaining it.[24] *Carpenter*, 585 U.S. at 314 (quoting *Miller*, 425 U.S. at 442).

---

[23] The dissent also stresses that law enforcement could deduce the identity of individuals caught within the geofence. Diss. Op. at 63–64. But we fail to see how this is relevant. If law enforcement only observed the short-term movements of everyone caught within the geofence, then it does not matter whether it learned the identity of those people or not—it still did not invade anyone's privacy interest in the whole of their physical movements.

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

Unable to refute this point, the dissent tries a different tack. The dissent argues that *Beautiful Struggle* and *Knotts* are distinguishable because they involved observation of "strictly . . . *public* movements." Diss. Op. at 94. According to the dissent, the duration of the government surveillance is only relevant in cases involving a person's public movements. But this case, unlike *Beautiful Struggle* and *Knotts*, involves technology with the capacity to surveil a person's *private* movements, too. So the dissent would apply a different set of principles here and treat the duration of the intrusion as basically irrelevant.

The dissent is correct that the government conducts a search when it uses sense-enhancing technology to learn information from inside a private space that it could not have learned without physically intruding on that space. *See Kyllo*, 533 U.S. at 34; *Karo*, 468 U.S. at 713–18. But the dissent fails to mention that those cases involved challenges brought by people who had a reasonable expectation of privacy *in the place searched*. *Kyllo*, 533 U.S. at 29–31; *Karo*, 468 U.S. at 714 ("This case thus presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights *of those who have a justifiable interest in the privacy of the residence*. . . . [W]e think that it does." (emphasis added)). By contrast, the Supreme Court has long held that someone who does not have a Fourth Amendment interest in the place or thing searched lacks standing to challenge that search. *Rawlings*, 448 U.S. at 104–06; *see Karo*, 468 U.S. at 716 n.4, 719 (distinguishing *Rawlings* because several defendants had a privacy interest in the place searched, unlike in *Rawlings*). So to challenge the government's use of technology to invade a protected space, a defendant must prove that the government violated *his* reasonable expectation of

privacy in that space. The mere fact that the government observed him behind closed doors is insufficient to confer Fourth Amendment standing.

Chatrie does not allege that the Location History data obtained by the government invaded his constitutionally protected space, like his home.[25] And to the extent that it may have showed him or others in *someone else's* protected space, Chatrie lacks standing to assert that person's potential Fourth Amendment rights. The dissent may be willing looking past these basic Fourth Amendment standing principles, but we are not.[26]

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

---

[25] Again, we take no position on whether this would be a search, since this issue is not properly presented here. But we do note that the answer isn't as obvious as the dissent represents that it would be. *Compare Karo*, 486 U.S. at 713–18, *with California v. Ciraolo*, 476 U.S. 207, 213 (1986) (holding that no search occurs when officers use technology to peer into a person's curtilage if the person knowingly exposes his curtilage's contents to others), *and Lewis v. United States*, 385 U.S. 206, 211 (1966) (holding that no search occurs when a person invites someone into his home who turns out to be a law enforcement informant).

[26] Adopting the dissent's sweeping approach would create a bizarre incongruity with other areas of Fourth Amendment doctrine. Under traditional Fourth Amendment principles, if the police physically entered Journey Christian Church without a warrant in search of Chatrie, he would not have standing to challenge that search (assuming he had no privacy interest in the church). But under the dissent's view, if police digitally "entered" that same church via Location History, Chatrie could challenge this as an invasion of his rights. For a view that claims to champion "historical understandings" of the Fourth Amendment, Diss. Op. at 46 (quoting *Carpenter*, 585 U.S. at 305), the dissent's approach actually eviscerates basic and longstanding Fourth Amendment principles.

But *Carpenter* did no such thing. As we have already explained, *Carpenter* did not cast aside everything that came before it and create a new framework for assessing Fourth Amendment violations. Rather, the Court concluded that access to at least 7 days' worth of CSLI invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements. *Carpenter*, 585 U.S. at 310–13. It then considered whether the third-party doctrine applied to CSLI and ultimately "decline[d] to extend" it, given the sensitive nature of that information and the fact that it is not voluntarily exposed to wireless carriers. *Id.* at 313–16. Yet Court did not overturn the third-party doctrine, nor did it rule out the possibility of it applying to other types of information or technology that fit more comfortably within its domain. *Id.* at 316. And it certainly did not reduce the doctrine to one factor in a totality-of-the-circumstances balancing inquiry.[27]

Here, we find that Chatrie—unlike Carpenter—did voluntarily expose his Location History to Google. So we conclude that the third-party doctrine applies to this case. But the dissent disagrees and identifies three facts that supposedly make Chatrie's disclosure of his Location History information not "meaningfully voluntary." Diss. Op. at 69. First, Location History, once enabled, always generates and collects information, so its collection

[27] The dissent's reading is only plausible because it creatively rearranges *Carpenter* to say something it never did. According to the dissent, *Carpenter* first "declin[ed] to extend the third-party doctrine," Diss. Op. at 48, then applied its "new framework" to recognize Carpenter's privacy interest, *id.* at 48–49, and finally considered voluntariness as a sort of independent factor, *id.* at 49. But this is not at all how the Court proceeded. Rather, it first recognized that access to 7 days' worth of CSLI invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements, 585 U.S. at 310–13, and then declined to extend the third party doctrine, partly because Carpenter's conveyance of CSLI was not meaningfully voluntary, *id.* at 313–16.

is even more automatic and less voluntary than the CSLI collected in *Carpenter*. Second, many individuals generate Location History data, so they must do so involuntarily. Third, Google does not "meaningfully inform" users of how it collects data or how much data it collects at the opt-in stage. *Id.* at 74. We address each argument in turn, finding none convincing.

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

Second, the fact that a large number of active Google users have enabled Location History does not prove that they use this service involuntarily. We agree with the dissent that "the use of technology is not per se voluntary just because the adoption of that technology is not as ubiquitous as the cell phone." Diss. Op. at 72. But the flip-side is also

[28] Nor is the absence of a "physical conveyance," like those in *Smith* and *Miller*, a meaningful distinction. Diss. Op. at 71. Someone who invites another to follow him around and record his movements has conveyed his location information just as voluntarily as someone who records every movement himself and gives the record to another.

true: The ubiquitous use of a particular technology does not necessarily mean that it is used involuntarily. And absent some explanation for why Location History is "'such a pervasive and insistent part of daily life' that [activating it] is indispensable to participation in modern society," *Carpenter*, 585 U.S. at 315 (quoting *Riley*, 573 U.S., at 385), we see no reason to treat it as such.[29]

Finally, Google provides adequate information at the opt-in stage to enable a user to knowingly consent to the collection of his data. Before a user can activate Location History, Google explains that "Location History saves where you go with your devices," that "Google regularly obtains location data from your devices," and that "[t]his data is saved even when you aren't using a specific Google service, like Google Maps or Google search." J.A. 1565. By choosing to opt in, then, a reasonable user would understand that he gave Google broad authorization to track and save Location History data whenever he goes anywhere with his device, even while he is not using it. A user who accepts those terms cannot later claim he did not knowingly expose his information simply because Google didn't explain *exactly* how accurately it would save where he went or *exactly* how regularly it would obtain location data. *Cf. Smith*, 442 U.S. at 745 ("The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not[,] in our view, make any constitutional difference."); *Florida v.*

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

Jimeno, 500 U.S. 248, 251 (1991) (holding that officers didn't exceed the scope of consent when suspect told them they could search the entire car and they searched containers within the car).[30]

The dissent warns that courts must exercise "humility" when adapting the Fourth Amendment to modern innovations. Diss. Op. at 103. But it is the dissent that fails to heed its own warning. Instead of faithfully apply established principles to the case before us, the dissent would have us depart from binding case law and apply a novel, unwieldy multifactor balancing test to reach the dissent's preferred policy outcome. We decline the invitation. Our Fourth Amendment doctrine compels a clear result here. If one thinks that this result is undesirable on policy grounds, those concerns should be taken to Congress.

* * *

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

AFFIRMED.

[30] The dissent also laments that pausing and deleting Location History is "easier said than done," Diss. Op. at 76, but its evidence for this proposition is basically nonexistent. Other than alluding to generalized grievances about Location History by members of Congress, the media, and Norway's Consumer Protection Committee, the dissent relies on a single email from a Google employee, who suggested that deleting Location History data might be difficult. But the district court made no finding about "[w]hether the substance of this remark is true or not," J.A. 1342, and, absent any further evidence, there is no way to know whether this remark accurately reflects the difficulty of deleting Location History data.

WYNN, Circuit Judge, dissenting:

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

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

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

I.

At the heart of this appeal, the majority opinion concludes that the government has a virtually unrestricted right to obtain the Location Data History of every citizen. But I believe the government needs a warrant to obtain such Location History data. And that's

something the government itself apparently believed at the time it conducted the respective intrusion, since it sought and obtained a warrant in this matter.[1]

A.

Ratified in 1791, the Fourth Amendment safeguards the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," by generally requiring the government to first obtain a warrant from a neutral judge or magistrate before conducting a search. U.S. Const. amend. IV. Historically, the Supreme Court interpreted the Fourth Amendment with an eye toward its origin as the embodiment of the Framers' desire to protect citizens from the arbitrary searches they endured under British rule. *See Carpenter v. United States*, 585 U.S. 296, 303–04 (2018). Consistent with this historical view, early decisions employed the "trespass doctrine," under which only physical intrusions by the government into private spaces constituted Fourth Amendment searches that required a warrant. *Katz v. United States*, 389 U.S. 347, 353 (1967) (internal quotation marks omitted); *see Carpenter*, 585 U.S. at 304; *Olmstead v. United States*, 277 U.S. 438, 457 (1928) (applying trespass doctrine), *overruled by Katz*, 389 U.S. at 347.

Justice Harlan's concurring opinion in *Katz v. United States* signaled a transition

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

from these early principles to modern Fourth Amendment jurisprudence.[2] His opinion articulated a "reasonable expectation of privacy" standard for what type of surveillance constitutes a Fourth Amendment search. *Katz*, 389 U.S. at 361–62 (Harlan, J., concurring). Under this standard, a Fourth Amendment search occurs if (1) an individual has an actual (subjective) expectation of privacy in some activity, and (2) that expectation is one that society recognizes as objectively reasonable. *Id.* at 361 (Harlan, J., concurring). Hence, any government surveillance that infringes upon a person's reasonable privacy expectation necessitates a warrant. *Katz* thereby expanded the recognized Fourth Amendment protections beyond mere physical intrusions. *Id.* at 353; *accord Desist v. United States*, 394 U.S. 244, 250 (1969) ("*Katz* for the first time explicitly overruled the 'physical penetration' and 'trespass' tests enunciated in earlier decisions of this Court."), *abrogated on other grounds by Griffith v. Kentucky*, 479 U.S. 314 (1987).

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

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

The seminal third-party-doctrine cases are *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 the phone numbers the suspect dialed on his home phone. *Smith*, 442 U.S. at 737–38. And in *Miller*, police accessed the suspect's bank records, such as checks and deposit slips. *Miller*, 425 U.S. at 437–38. In those cases, the Supreme Court held that the suspects had no reasonable privacy expectations in the records in question because the documents were unrevealing business records that the suspects had voluntarily conveyed to third parties. *See Smith*, 442 U.S. at 737, 740–42; *Miller*, 425 U.S. at 442–43.

The analysis in those cases was twofold and found its roots in Justice Harlan's *Katz* concurrence. First, *Smith* and *Miller* reasoned that individuals have no subjective privacy expectation in the phone numbers they dial or in their bank records because the "nature of those records" is that they are "business records" that reveal little personal information. *Carpenter* 585 U.S. at 308–09 (first citing *Smith*, 442 U.S. at 742–43; and then citing *Miller*, 425 U.S. at 440–43). The Court in *Smith*, for instance, stressed the pen registers' "limited capabilities": the pen registers did "not acquire the contents of communications," nor reveal the caller and call recipient's "identities, nor whether the call was even completed." *Smith*, 442 U.S. at 741–42 (emphasis omitted); *accord Miller*, 425 U.S. at 440, 442 (stating that the records were "not confidential communications but negotiable instruments . . . in commercial transactions").

Second, and relatedly, the Court held in both cases that society did not recognize a "reasonable" (or objective) privacy expectation in such unrevealing business records that individuals voluntarily provide to third parties. *See Carpenter*, 585 U.S. at 309 ("When

Smith placed a call, he voluntarily conveyed the dialed numbers . . . by exposing that information . . . in the ordinary course of business." (quoting *Smith*, 442 U.S. at 744 (cleaned up))); *Miller*, 425 U.S. at 443.

Nevertheless, *Smith* qualified its analysis with an eye toward the future. It specified that, if a day should come when our subjective expectations of privacy change due to "influences alien to well-recognized Fourth Amendment freedoms," then the subjective-expectation requirement would have "no meaningful role" in ascertaining the bounds of the Fourth Amendment. *Smith*, 442 U.S. at 740 n.5. Instead, "a normative inquiry would be proper." *Id.* Likewise, Justice Marshall's dissent in *Smith* voiced an argument that *Carpenter* would later echo: disclosure to a phone company or bank is not meaningfully voluntary in modern society. *See id.* at 749–51 (Marshall, J., dissenting).

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

In so holding, the Court stressed that the beeper was a rudimentary technology that merely "augment[ed]" the visual "sensory faculties" that officers had at "birth." *Id.* at 282, 285. Thus, *Knotts* "was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance." *Carpenter*, 585 U.S. at 306. *Knotts*, like *Smith*, also turned an eye to the future: the Court presciently qualified that should "twenty-four hour surveillance of any citizen" become "possible," then "different constitutional principles may be applicable." *Id.* at 306–07 (quoting *Knotts*, 460 U.S. at 283–84 (cleaned up)).

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

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

However, as technology quickly advanced in the ensuing decades and enabled police to surreptitiously collect unprecedented levels of information, the Supreme Court began curtailing the third-party and public-surveillance doctrines to ensure that the

exceptions to the Fourth Amendment's protections did not swallow the whole. In doing so, the Supreme Court ensured that the Fourth Amendment remained a firm bulwark against government overreach.

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

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

conducted with more precise and comprehensive technology. *See id.* at 415–16 (Sotomayor, J., concurring); *id.* at 427–30 (Alito, J., concurring in the judgment).

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

For the fifth concurring justice, Justice Sotomayor, even a *short-term* GPS search violated a reasonable privacy expectation because the technology's "unique attributes" set it apart from the rudimentary beeper in *Knotts*. *Id.* at 415 (Sotomayor, J., concurring). Most famously, she reasoned that because GPS technology "generates a precise, comprehensive record" of a person's public movements, it "reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," which violates our deepest privacy expectations. *Id.* Justice Sotomayor further pointed out that a short GPS search is cheaper, easier to use, and more concealable than conventional surveillance methods—attributes that allow technologies like GPS to "evade[] the ordinary checks that constrain abusive law enforcement practices." *Id.* at 416. Additionally, she noted, GPS technology permits the government to "store" and "efficiently mine" records of an individual's movements "years into the future." *Id.* at 415. For these reasons, she warned, even a short

GPS search could chill First Amendment freedoms and "alter the relationship between citizen and government in a way that is inimical to democratic society." *Id.* at 416 (quotation omitted). Finally, she lamented that the third-party doctrine is "ill suited to the digital age," in which people reveal intimate information during "mundane tasks" without expecting their devices to enable "covert surveillance of their movements." *Id.* at 417 & n.*.

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

Thus, in each of these seminal cases, the Supreme Court grappled with how to maintain constitutional privacy protections against police use of or access to encroaching technologies. And, in the majority opinions in most of these cases and in the *Jones* concurrences, the Court recognized that traditional Fourth Amendment principles were ill-suited to combating the realities of modern technology.

B.

All this case law, demonstrating the Court's growing recognition of the profound impact of technological advancements on Fourth Amendment rights, led up to the Court's

2018 decision in *Carpenter v. United States*. While building on all that came before it, *Carpenter* marked a "[s]ea [c]hange" in Fourth Amendment jurisprudence as it pertains to "a person's digital information." Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 Harv. L. Rev. 1790, 1799–1800 (2022) [hereinafter Tokson, *The Aftermath of* Carpenter].

In *Carpenter*, the Court held that a police intrusion into seven days of the defendant's historical cell-site-location-information ("CSLI") records, which produced two days' worth of data, constituted a Fourth Amendment search. *Carpenter*, 585 U.S. at 302, 313. 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 companies, *id.* at 306, 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. In other words, the Sixth Circuit took a view very similar to that of the majority here, asking only whether the information in question had been voluntarily conveyed in some manner to a third party.

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

The *Carpenter* Court began by reiterating the *Katz* test: the Fourth Amendment protects against intrusion into the sphere in which an individual has a reasonable expectation of privacy. *Id.* at 304. It then explained that, while "no single rubric" defines what constitutes a reasonable privacy expectation, the Court's analysis must always be "informed by historical understandings of what was deemed an unreasonable search when the Fourth Amendment was adopted." *Id.* at 304–05 (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 it has kept those "Founding-era understandings in mind" when considering "innovations in surveillance tools." *Id.* Pointing to the examples of *Kyllo* and *Riley*, detailed above, the Court explained that its Fourth Amendment jurisprudence has evolved in step with technological developments: "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to [preserve historical privacy protections]." *Id.* (quoting *Kyllo*, 533 U.S. at 34) (cleaned up); *see id.* (noting that the Court "rejected in *Kyllo* a 'mechanical interpretation' of the Fourth Amendment" to protect individuals from advancing technology (quoting *Kyllo*, 533 U.S. at 35)); *id.* (pointing to its "recogni[tion]" in *Riley* that "the 'immense storage capacity' of modern cell phones" rendered a cell phone search

fundamentally different from a traditional, physical search of an arrestee's person (quoting *Riley*, 573 U.S. at 393)).

With that background, the Court turned to consider the CSLI intrusion at bar. It quickly concluded that the sort of digital data at issue—"personal location information maintained by a third party"—"does not fit neatly" into any existing line of Fourth Amendment jurisprudence. *Id.* at 306. Instead, this data "lie[s] at the intersection" of the third-party doctrine (*Smith* and *Miller*) and public-surveillance cases (*Knotts* and *Jones*). *Id.* Both lines of cases would seemingly "inform our understanding of the privacy interests at stake," *id.*, but neither squarely applies because this kind of data constitutes a "qualitatively different category" of information, *id.* at 309.

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

dialed digits, but a detailed and comprehensive record of the person's movements." *Id.* at 309.

In so declining to extend the third-party doctrine, the Court rejected the notion that there is "a straightforward application of [that] doctrine" to police use of data like CSLI. *Id.* at 314. To the contrary, the Court held that applying the third-party doctrine to the CSLI in *Carpenter* would have constituted "a significant extension of [the doctrine] to a distinct category of information." *Id.* Accordingly, it warned that courts would be remiss to "mechanically" apply old theories like the third-party doctrine to novel records like CSLI. *Id.* ("In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.").

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

maintained a reasonable privacy expectation in his CSLI data, and so the intrusion constituted a Fourth Amendment search. *Id.* at 313.

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

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

Leading scholars agree that *Carpenter* created a factor-based test derived from those considerations, though they disagree on which factors are the most important or mandatory. *E.g.*, Paul Ohm, *The Many Revolutions of* Carpenter, 32 Harv. J.L. & Tech. 357, 363, 369 (2019) (recognizing *Carpenter* created "new, multi-factor test" to analyze an individual's reasonable privacy expectation against intruding technology and "herald[ed] a new mode of Constitutional analysis"); Susan Freiwald & Stephen W. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 Harv. L. Rev. 205, 219 (2018) (multifactor

analysis was "clearly central" to the Court's holding); Tokson, *The Aftermath of* Carpenter, *supra*, at 1830 (describing the "*Carpenter* factors" and concluding from a survey of cases that "[a] multifactor *Carpenter* test has begun to emerge from the lower court[s]"). In reaching this conclusion, scholars rely on the Court's analysis and its concluding sentence, which reads: "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Carpenter*, 585 U.S. at 320. In my view, such a factor-based examination is the correct interpretation of the Court's opinion.

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

This rationale reflects the Court's understanding that rapid technological advances have created shifts "in kind and not merely in degree from the technology of the past." *Ohm*, *supra*, at 399. These shifts required the Court to adjust its analysis of the Fourth

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

Put simply, the Court declined to extend existing doctrines to exempt CSLI from Fourth Amendment protections based on the principle that it first recognized decades earlier: previously unimaginable technology that reveals unprecedented amounts of personal information requires new rules. *Carpenter*, 585 U.S. at 310–14 (citing the *Jones* concurrences and rejecting the "mechanical" application of old doctrines); *accord Riley*, 573 U.S. at 393 (stating that comparing a physical search to a cell phone search is like "saying a ride on horseback is materially indistinguishable from a flight to the moon"). Thus, "[t]he beating heart" of *Carpenter* "is its deep and abiding belief in the exceptional nature of the modern technological era." Ohm, *supra*, at 399.

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

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

revealed about the defendant); *Ohm*, supra, at 386 (explaining that *Carpenter* adopted a normative analysis of each factor that focused on the capabilities of CSLI as a category of information).

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

II.

A.

A faithful reading of *Carpenter*—not to mention common sense—compels the conclusion that when the police obtained Chatrie's Location History data, they engaged in a Fourth Amendment search. That conclusion is evident upon evaluating how the *Carpenter* factors apply to the Location History intrusion in this case.

1.

The first factor that *Carpenter* identified was the comprehensiveness of the intrusion, focusing on CSLI's near-perfect surveillance capabilities. *Carpenter*, 585 U.S. at 311–12. The Court looked at this factor from two dimensions: the depth and the breadth of the intrusion.

Regarding depth, the data collected in this case and in *Carpenter* was extremely comprehensive, involving a deep intrusion into each user's privacy rights. But the intrusion

into Chatrie's Location History was even more comprehensive than the intrusion in *Carpenter* because Location History is collected more often and is more precise than CSLI as described in *Carpenter*.

In *Carpenter*, the Court was concerned that CSLI provided "near perfect surveillance" of its owner and created a "detailed, encyclopedic, and effortlessly compiled" record. *Id.* at 309. The *Carpenter* Court concluded that the CSLI intrusion provided nearly perfect surveillance because, unlike police tracking of a vehicle—which a person exits and which remains parked outside—a cell phone remains permanently attached to its owner and "faithfully follows" them into private areas. *Id.* at 311–12 ("A cell phone—almost a 'feature of human anatomy'—tracks nearly exactly the movements of its owner." (citation omitted) (quoting *Riley*, 573 U.S. at 385)); *see id.* at 311 (noting many people even use their cell phones in the shower).

So too here. As with CSLI, Location History tracks a smartphone's location, so it likewise provides "near perfect surveillance" of its user. *Id.* at 311–12. And like CSLI, Location History is collected with sufficient frequency to be able to faithfully track the user's movements.

Location History, however, provides even more detailed surveillance than CSLI because it is collected much more often. In *Carpenter*, CSLI only captured Carpenter's location when he affirmatively placed or received a call—no call, no data. *Id.* at 302. But the Court also recognized that in recent years, companies had begun collecting CSLI from other "routine data connections." *Id.* at 301. In line with its normative approach, the Court considered those advancements in its analysis, stating that with CSLI, the suspect has

"effectively been tailed every moment of every day for" as long as the company maintained its records (in that case, five years). *Id.* at 312.

While the "every moment" description was not accurate to Carpenter's own CSLI data—and was likely at least a slight exaggeration even considering the advancements in CSLI technology by the time of the *Carpenter* decision[3]—it *does* essentially capture what we know of Location History data because that technology *automatically tracks users every two minutes*. *United States v. Chatrie*, 590 F. Supp. 3d 901, 908 (E.D. Va. 2022). So with Location History, police can reconstruct a user's movements with startling precision. The numbers in this case bear this out: through Location History, the police were able to collect an average of about 76 data points on each person surveilled *in just two hours*. Compare that to CSLI, which collected only about 101 data points on Carpenter *in a full day*. *Carpenter*, 585 U.S. at 302. Thus, Location History data is even more "detailed, encyclopedic, and effortlessly compiled" than CSLI. *Id.* at 309.

Additionally, Location History implicates even deeper privacy concerns than the CSLI in *Carpenter* because not only does it collect far more data points about each user, but also it is markedly more *precise*. In *Carpenter*, the data placed the defendant within a "wedge-shaped sector," *id.* at 312, that ranged from "a dozen" to "several hundred" city

[3] According to *Carpenter*, "[w]hile carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections." *Carpenter*, 585 U.S. at 301. The opinion does not clarify how frequently the collection of data from "routine data connections" occurs.

blocks and was "up to 40 times more imprecise" in rural areas, *id.* at 324 (Kennedy, J., dissenting) (noting CSLI is even less precise than GPS).

Here, by contrast, the district court found that "Location History appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing location data." *Chatrie*, 590 F. Supp. 3d at 907. In fact, Location History can hunt down a user's whereabouts within *meters*, and even discern elevation, locating the specific *floor in a building* where a person might be. *Id.* at 908–09.

Most critically, it is a fundamental legal principle that any intrusion into a constitutionally protected space receives Fourth Amendment protection. *E.g.*, *Karo*, 468 U.S. at 714–15 (search occurred where government monitored a beeper inside "a private residence, a location not open to visual surveillance"); *Kyllo*, 533 U.S. at 33–35 (search occurred where government used device to monitor radiation through home's walls). And Location History data is so granular that it can pinpoint and continuously follow a device inside protected spaces. For example, the geofence in this case covered over 17 acres and encompassed a nearby church. *Chatrie*, 590 F. Supp. 3d at 918. The district court found that the geofence could have also captured a hotel, "several units of [an] apartment complex," "a senior living facility," and "what appear to be several residences" for one hour at Step One, and it had *no* geographic limits for an additional hour in Step Two.[4] *Id.*

[4] As a reminder, Step One of the geofence warrant "'compel[led] Google to disclose a de-identified list of all Google users' whose Location History data indicates were within the geofence during a specified timeframe." *Chatrie*, 590 F. Supp. 3d at 914–15 (cleaned up). At Step Two, law enforcement could compel Google to provide additional location information for a narrowed list of users "*beyond* the time and geographic scope of the (Continued)

at 923. It appears nearly impossible to limit geofences to public spaces because Location History can inaccurately sweep more ground than police requested,[5] and Google does not set geographic limits on Step Two in standard geofence warrants. *Id.* at 916, 922–23.

Consequently, every geofence in a developed area could potentially reveal information "that could not otherwise have been obtained without physical intrusion into a constitutionally protected area." *Kyllo*, 533 U.S. at 34 (internal quotation marks omitted); *see, e.g.*, Jake Snow, *Cops Blanketed San Francisco In Geofence Warrants. Google Was Right to Protect People's Privacy*, ACLU of N. Cal. (Jan. 7, 2024), https://www.aclunc.org/blog/cops-blanketed-san-francisco-geofence-warrants-google-was-right-protect-peoples-privacy [https://perma.cc/2Y7S-DRBG] (analyzing all geofence warrants from January 2018 to August 2021 in San Francisco and finding that—in that area alone—the geofences covered hundreds of residences, twelve places of worship, seven medical sites of care, and other private spaces). That crosses a "bright" line: police need a warrant. *Kyllo*, 533 U.S. at 40.

---

original request." *Id.* at 916. Google "imposes no geographical limits on this Step 2 data." *Id.* (quotation marks omitted).

Additionally, Google has no "firm policy as to precisely *when* a Step 2 request [has] sufficiently narrow[ed]" the list of users captured in Step One for whom police could request more data at Step Two. *Id.*

[5] While Location History is more precise than CSLI, it is not infallible. The district court found that the "largest confidence interval" for a user located within the geofence had a radius of roughly 387 meters—more than twice as large as the geofence. *Chatrie*, 590 F. Supp. 3d at 922–23. Thus, the court found that the "Geofence Warrant *could* have captured the location of someone who was hundreds of feet outside the geofence." *Id.* at 922. The court found that the government did not craft the geofence to account for these inaccuracies. *Id.* at 930–31.

The majority opinion dismisses this concern, concluding that even though the instant geofence intrusion did surreptitiously enter several constitutionally protected spaces—including residences—this issue must be saved for future cases because the intrusion did not actually enter Chatrie's home, and he therefore lacks Fourth Amendment standing to challenge it on that ground.[6] Maj. Op. at 19 n.17, 30–31, 31 n.26. But that analysis is incorrect. The rules are simple: a person has Fourth Amendment standing if they have a reasonable expectation of privacy in the thing searched. Whether a person has a reasonable expectation of privacy in certain data is *inextricable from the data's capabilities*.

Citizens have a fundamental privacy expectation in non-public spaces, particularly their homes. *E.g.*, *Kyllo*, 533 U.S. at 34; *Karo*, 468 U.S. at 714–15. Accordingly, all citizens would reasonably expect privacy in data that continuously and retrospectively tracked their movements in these protected spaces with remarkable precision, even locating the specific room they occupy within a secure area.

It follows then that Chatrie would have a reasonable expectation of privacy from such an intrusion that could capture a church and residences at Step One and was boundless at Step Two. *Chatrie*, 590 F. Supp. 3d at 914–16. Indeed, police executed a search that *would* have captured Chatrie's home or other constitutionally protected space if it was in the Step One boundary, or if he happened to travel there during Step Two. It does not matter

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

that Chatrie *happened* to stay outside of constitutionally protected spaces during a search that would have otherwise captured those spaces. *See Arizona v. Hicks*, 480 U.S. 321, 325 (1987) ("A search is a search, even if it happens to disclose nothing but the bottom of a turntable.").

The *Kyllo* majority rejected the similar argument that the search of heat waves emanating from the home did not implicate the Fourth Amendment if the search did not catch more intimate information. That argument, Justice Scalia explained, was not only "wrong in principle," but also "impractical" because "no police officer would be able to know in advance" whether his surveillance will "pick[] up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." *Kyllo*, 533 U.S. at 38–39. Likewise, here, when police executed an intrusion that would capture private spaces, they had no crystal ball to predict whether Chatrie would enter those spaces during the intrusion.

It was also the case in *Carpenter* that no facts showed that the CSLI intrusion entered the defendant's own protected spaces. But that did not affect his standing. The Court simply held that because the CSLI intrusion had the capability to follow the defendant into any of numerous sorts of sensitive spaces, the intrusion was unlawfully intimate. *Carpenter*, 585 U.S. at 311 ("A cell phone faithfully follows its owner *beyond public thoroughfares* and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." (emphasis added)). That is, the Court focused on the surveillance tool's *capabilities* during the intrusion as opposed to the specific facts of each intrusion. Because an intrusion into two days' worth of Carpenter's CSLI data met

the *Carpenter* factors, Carpenter had a reasonable privacy expectation in that data and thus had standing. In so holding, the *Carpenter* Court affirmatively instructed lower courts to consider the potential reach of each intrusion, without regard to whether the intrusion indeed invaded the defendant's own private space under traditional Fourth Amendment standing principles. *Id.* The government thus cannot circumvent the Constitution merely because, by sheer luck, its target did not stray from the safe zone.

In short, the intrusion into Chatrie's Location History satisfies the depth portion of *Carpenter*'s first factor because it provides nearly perfect surveillance of its owner and creates a "detailed, encyclopedic, and effortlessly compiled" record of the owner's movements. *Id.* at 309. And the intrusion was so broad that it did in fact enter private areas. This factor weighs strongly in favor of holding that the police conducted a Fourth Amendment search.

2.

Next is the intrusion's breadth (the second part of factor 1), which should be considered alongside its retrospective capabilities (factor 2) because the two are related.

Regarding breadth, the *Carpenter* Court was particularly concerned that wireless companies retained CSLI data for five years and stored that information for millions of people. This consideration was intertwined with the retrospective quality of the data: that is, because the wireless companies retained CSLI data for five years, police could "reconstruct a person's [past] movements," such that the person "has effectively been tailed every moment of every day for five years." *Id.* at 312; *see id.* at 313 ("[S]eismic shifts in

digital technology . . . made possible the tracking of not only Carpenter's location but also everyone else's . . . for *years and years*." (emphasis added)); *id.* at 315 (same).

This breadth deviated from historical privacy expectations, leading the Court to conclude the data was therefore qualitatively different from data the Court had previously concluded did not implicate the Fourth Amendment. *Carpenter* highlighted that police historically could not "reconstruct a person's [past] movements" without facing "a dearth of records and the frailties of recollection." *Id.* at 312. But with CSLI, police could "travel back in time to retrace a person's whereabouts" with precision, not only in the recent past, but going back years. *Id.* Not only that, but CSLI data was also available for "400 million devices in the United States"—not just those of suspects—so "this newfound tracking capacity runs against everyone." *Id.* Unlike with the trackers in *Knotts* or *Jones*, "police need not even know in advance whether they want to follow a particular individual [using CSLI], or when." *Id.*

Location History raises the same breadth and retrospectivity concerns: at the time of the geofence intrusion at issue here, Google collected and retained Location History records from the time Location History was enabled, which could have taken place years prior. This means that the data obtained in a geofence intrusion is pulled from a preexisting database of users' past movements, empowering police to time travel for each intrusion. Thus, each user has "effectively been tailed" since they activated Location History. *Id.*; *see also Chatrie*, 590 F. Supp. 3d at 909. Plus, like CSLI, Location History data is available for "numerous tens of millions" of unsuspecting Google users. *Chatrie*, 590 F. Supp. 3d at 907.

Yet, geofence intrusions are even broader than the intrusion in *Carpenter* because there is *no* limit on the number of users police can include in a geofence. With CSLI, police at least had to provide a specific phone number to search, so they had to identify a criminal suspect before they could pry into his or her historical CSLI data. By stark contrast, geofence intrusions permit police to rummage through the historical data of an unlimited number of individuals, *none* of whom the police previously identified nor suspected of any wrongdoing. Indeed, the very *point* of the geofence intrusion is to identify persons whose existence was unknown to police before the search.

Geofence intrusions are accordingly low-value fishing expeditions. So, even when police *do* obtain a warrant for a geofence, such a warrant is uncomfortably akin to the sort of "reviled" general warrants used by English authorities that the Framers intended the Fourth Amendment to forbid. *Carpenter*, 585 U.S. at 303 (quoting *Riley*, 573 U.S. at 403) (describing roots of the Fourth Amendment); *see also Steagald v. United States*, 451 U.S. 204, 220 (1981) ("The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." (citations omitted)). Now that the majority has eliminated the warrant requirement in cases like this one, police do not even need to "specif[y] . . . an offense" before they can conduct a geofence intrusion. *Id.*

It follows that the breadth portion of the first factor (comprehensiveness) and the second factor (retrospectivity) weigh in favor of concluding that the geofence intrusion in this case was a search under *Carpenter*.

3.

Turning to the third factor, intimacy, *Carpenter* concluded that because CSLI captured "near perfect surveillance," it uncovered information that was personally revealing and thus intimate. *Carpenter*, 585 U.S. at 312. As a result, this factor also favored the conclusion that the Fourth Amendment applied. *Id.* at 311–12. The same is true here.

Just like CSLI, Location History provides near-perfect surveillance, enabling the government to reconstruct a "detailed and comprehensive record of [Chatrie's] movements" for two hours. *Id.* at 309. The government could learn a great deal about Chatrie in those two hours: the geofence intrusion occurred in "a busy part of the Richmond metro area" between 3:50 pm and 5:50 pm. *Chatrie*, 590 F. Supp. 3d at 919, 925. That is when most people leave work or school and travel to their next destinations, carrying their phones into intimate spaces and engagements. A two-hour search could tour a person's home, capture their romantic rendezvous, accompany them to any number of medical appointments, political meetings, strikes, or social engagements, or otherwise begin constructing their afternoon and early-evening routines. *See* J.A. 145 (Google LLC's amicus brief filed in the district court, arguing that its users maintain a reasonable expectation of privacy in their Location History against a geofence intrusion, for there is "nothing limited" about a 2-hour geofence intrusion).

This is not a mere supposition. At the suppression hearing, Chatrie's defense counsel demonstrated that the identities of innocent users caught up in the geofence were easily deduced from the anonymized data that Google provided in Step 2. *Chatrie*, 590 F. Supp. 3d at 923–24. To make this showing, the defense took three users who were caught

in the geofence—that is, innocent individuals who just happened to be near the site of the robbery—and demonstrated that the data the police received from Google pursuant to its warrant retroactively tailed those individuals into private spaces: all three traveled to or from residences, one traveled to a school, and one traveled to a hospital. *Id.* at 923. Chatrie's expert also showed how deductions from this information allowed him to easily uncover those individuals' identities. *Id.* at 923–24.

And, as noted above, it does not matter whether the intrusion here revealed intimate information about Chatrie personally. *Carpenter* did not mention any facts that the CSLI search revealed about the defendant in that case—rather, the Court assessed only whether the search *could* reveal intimate information unrelated to legitimate police needs. *Carpenter*, 585 U.S. at 311. The search here certainly could—and did.

Simply put, there can be no doubt that "[a]s with [the] GPS information" in *Jones*, or the CSLI in *Carpenter*, "the time-stamped data" from a geofence intrusion "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious and sexual associations.'" *Id.* at 311 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)); *accord Smith*, 442 U.S. at 751 (Marshall, J., dissenting) (recognizing that because people "value" privacy in basic activities, "the prospect of unregulated governmental monitoring [related to which phone numbers they dial] will undoubtedly prove disturbing even to those with nothing illicit to hide"). Additionally, because the geofence intrusion could enter constitutionally protected spaces, it by default could reveal intimate information. *Kyllo*, 533 U.S. at 37.

It is also of little importance that the intrusion here was of a shorter duration than in *Carpenter*. The government in *Carpenter* conducted two intrusions: it requested records of Carpenter's movements over both a seven- and 152-day period, which respectively revealed two and 127 days of data. *Carpenter*, 585 U.S. at 302. The Court stated that the 127 days of data provided an "intimate window into a person's life" that revealed the litany of associations that Justice Sotomayor identified in her *Jones* concurrence. *Id.* at 311 (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). But the 127-day figure was nowhere near outcome-determinative: *Carpenter* ultimately held that only *two days* of CSLI data was intimate enough to constitute a search. *Id*. at 310 n.3. Even the two-day figure is not dispositive because the Court expressly limited its holding to the facts before it, and thus did not address whether a shorter search would invoke constitutional scrutiny. *Id.* Moreover, the Court's intimacy analysis relied on Justice Sotomayor's concurrence in *Jones*, which argued that *short-term* searches are no less intimate by virtue of their limited duration. *See id.* at 311 (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

Indeed, *Carpenter* only mentioned two temporal periods in the main text of the opinion—it stressed repeatedly that CSLI records and stores data for "years," *id.* at 312, 313, 315, 319, and concluded that tracking over "127 days" creates a comprehensive record, *id.* at 311—while holding in a footnote that the much shorter duration of *two days* of data collection still constituted a search, *id.* at 310 n.3. So, the Court clearly focused on the character of the search, rather than its length. Location History operates the same way: like CSLI, Location History records and stores data for years, and it likewise provides nearly perfect, comprehensive surveillance. Thus, the fact that the intrusion here lasted

only two hours does not preclude a finding that it revealed intimate information or constituted a search.

Finally, the majority opinion cites *Knotts* and this Court's en banc holding in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, in which this Court held that Baltimore's weeks-long aerial-surveillance program constituted a Fourth Amendment search. The majority relies on these cases for the principle that only prolonged tracking like that in *Beautiful Struggle*—as opposed to "short-term tracking of public movements" like in *Knotts*—implicates the Fourth Amendment. Maj. Op. at 26 (quoting *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021)). In the majority opinion's view, the geofence intrusion at bar is like the one-trip beeper intrusion in *Knotts*, and hence not a search. *Id.* at 19–20.

But the majority opinion's simplistic comparison to *Knotts* is inapt because it ignores the glaring differences between the beeper surveillance in *Knotts* and the vastly more sophisticated Location History technology here. Specifically, *Knotts* involved brief *real-time* public surveillance with a "rudimentary" technology that only augmented officers' natural-born senses. *Carpenter*, 585 U.S. at 306 (describing *Knotts*). By contrast, a geofence intrusion involves a retrospective (for years), continuous, nearly perfect surveillance technology, which enters private areas and captures information historically unavailable to uninvited human senses.

As elaborated on further below, *infra* at 93–97, *Knotts* and *Beautiful Struggle* involved the tracking of only *public* movements. Yet, as *Carpenter* held, intrusions into CSLI are categorically different from intrusions that only capture public movements. *See*

Carpenter, 585 U.S. at 311–12. For all the reasons I've explained, the same is true of the Location History data in this case. The geofence intrusion here was so broad that it could have followed users through dozens of non-public spaces, including residences, religious spaces, and senior living facilities. Thus, the intrusion did not merely constitute a "short-term tracking of *public* movements." *Beautiful Struggle*, 2 F.4th at 341 (emphasis added).

In sum, Location History can reveal intimate information about an individual, so the third *Carpenter* factor favors a finding that police obtaining Location History data must obtain a warrant.

4.

The fourth *Carpenter* factor, ease of access, also favors this conclusion. Geofences, like CSLI searches, are "easy, cheap, and efficient compared to traditional investigative tools." *Carpenter*, 585 U.S. at 311. As with CSLI, police conduct a geofence intrusion "[w]ith just the click of a button" that enables them to scour the continuous locations of numerous people in any area at any time—"at practically no expense." *Id.*; *see also* Ohm, *supra*, at 369 (noting that cell phone location tracking is almost twice as cheap as GPS tracking, while GPS tracking is 28 times cheaper for police than covert pursuits). In fact, geofence intrusions are remarkably "easy" because Google does most of the work *for* the police.

In considering this factor, *Carpenter* heeded the concerns raised in the *Jones* concurrences, which cautioned against enabling powerful leaps in police surveillance capabilities through practical advances. *See Jones*, 565 U.S. at 429–30 (Alito, J., concurring in the judgment) ("In the precomputer age, the greatest protections of privacy

were . . . practical."); *id.* at 416 (Sotomayor, J., concurring) (warning that government abuse would ensue from the unrestrained police power to use advanced and efficient, relatively low-cost technology). In his *Jones* concurrence, Justice Alito emphasized that if a digital search would have been exceptionally demanding and costly for police to replicate in the pre-digital age, then society does not reasonably expect that search to occur. *Id.* at 429–30 (Alito, J., concurring in the judgment). A geofence intrusion certainly would have been impossible to replicate in the pre-internet age. So, it violates society's privacy expectations.

The fourth factor therefore favors the conclusion that police engage in a search when they obtain geofence data.

5.

The final factor to consider is voluntariness. To be sure, it is unclear whether *Carpenter* requires us to consider voluntariness at all. That's because the Court expressly concluded that the defendant had a reasonable expectation of privacy in his CSLI records and that the third-party doctrine did not apply *before* it ever addressed voluntariness. *See Carpenter*, 585 U.S. at 313. However, in its summation at the end of the opinion, the Court stated that "[i]n light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and *automatic nature of its collection*, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Id.* at 320 (emphasis added). The reference to the "automatic nature of [the] collection" seemingly refers to voluntariness. This ambiguity is

expected: *Carpenter* deliberately left open to interpretation the precise contours of its analysis. *See, e.g.*, Tokson, *The Aftermath of* Carpenter, *supra*, at 1798, 1800.

At minimum, the *Carpenter* Court's discussion of voluntariness in a separate rebuttal section—after the Court had already concluded the intrusion was a search—establishes that it is the least important factor in the overall analysis. *See* Matthew Tokson, *Smart Meters as a Catalyst for Privacy Law*, 72 Fla. L. Rev. F. 104, 112 (2022) ("Most scholars view involuntariness not as a requirement but as merely one factor among many examined in *Carpenter*. The Court's discussion of the voluntariness issue . . . was mostly confined to a single paragraph in a lengthy opinion that largely focused on [other] factors[.]" (footnote omitted) (collecting scholarship)); Freiwald & Smith, *supra*, at 219 (observing that *Carpenter* established a multiprong test made up of only the four primary factors already discussed).

Assuming arguendo that voluntariness is a mandatory factor to be considered in the analysis of whether a police intrusion into digital records constitutes a search, it is clear for reasons explained below that Chatrie's sharing of Location History was *not* meaningfully voluntary. Additionally, even if this factor slightly leans in the government's favor, this factor's contribution is marginal and insufficient to sway the balance of the factor-based test.

Carpenter rejected an extension of the third-party doctrine to CSLI intrusions, noting that CSLI differs from the records in *Smith* and *Miller* in part because the conveyance of CSLI is involuntary. *Carpenter*, 585 U.S. at 315. That is, while *Smith* and *Miller* held that individuals had no reasonable privacy expectations in their bank records

and phone numbers dialed because they voluntarily (and often physically) conveyed those records to third-party companies, *Carpenter* reasoned that individuals do not "voluntarily" convey their CSLI data to third parties merely by using their cell phones—at least not in any "meaningful sense." *Id.*

In so concluding, the Court reasoned that cell phones are a ubiquitous part of modern life. And the Court reasoned that individuals convey CSLI to wireless companies by simply turning on their cell phones and connecting to the wireless network. After that, any cell phone activity generates CSLI.[7] *Id*. So, because cell phones are prevalent in modern society, and cell phone use necessarily creates CSLI without much action or awareness by the user, the Court concluded the conveyance of CSLI data is not "meaningful[ly]" voluntary. *Id.*

The sharing of Location History is likewise not "meaningful[ly]" voluntary. *Id.* First, like CSLI, once Location History is enabled, it is always generated and collected. In fact, Location History is even less voluntarily conveyed because it is conveyed automatically every two minutes, while CSLI is only conveyed when there is phone activity like an incoming text. And users are even less likely to be aware of the conveyance of Location History than they are CSLI because once users enable Location History, it is

[7] Again, the government in *Carpenter* only collected the defendant's CSLI data at the start and end of calls, and wireless companies likewise had long only collected CSLI data in those increments. *Carpenter*, 585 U.S. at 301, 302. But the Court recognized that "in recent years," companies had also begun collecting CSLI from the transmission of text messages and routine data connections. *Id.* at 301. Although those advancements did not apply to Carpenter himself, the Court considered them in its analysis of voluntariness.

automatically conveyed *across all devices* on which a user is logged into Google, even when the user has deleted the Google app through which they opted into Location History. Thus, the ongoing conveyance of Location History is more automatic and less voluntary than CSLI.

Compare that to the conveyances in *Smith* and *Miller*, in which individuals were much more aware that they were conveying information to third parties. In *Smith*, the individuals physically dialed each number they conveyed, and the phone company sent monthly bills listing some of the calls that the companies had collected. *Smith*, 442 U.S. at 742 (noting users "see a list of their long-distance (toll) calls on their monthly bills"). And of course, in *Miller*, individuals had to physically convey checks and deposit slips to the bank. *Miller*, 425 U.S. at 442; *e.g.*, Alyssa Bentz, *First in Online Banking*, Wells Fargo History (last visited Apr. 1, 2024), https://history.wf.com/first-in-online-banking/ [https://perma.cc/FRT2-XHRR] (noting that in 1984—eight years after *Miller* was decided—internet banking software had not been developed so customers "still had to input their [bank] transactions by hand"). The nature of such a physical conveyance differs drastically from a cell phone's automatic conveyance every two minutes.

Second, a substantial number of individuals generate Location History, just like CSLI. To be sure, Google's Location History service tracks fewer Americans than does CSLI. *Compare Chatrie*, 590 F. Supp. 3d at 907 (Google did not provide specific numbers but revealed it tracks "numerous tens of millions" of users), *with Carpenter*, 585 U.S. at 300 (noting that "[t]here are 396 million cell phone service accounts in the United States," which is greater than the number of people). And the majority contends that the fact "[t]hat

two-thirds of active Google users have not enabled Location History is strong evidence" that opting in is voluntary. Maj. Op. at 22.

But the use of technology is not per se voluntary just because the adoption of that technology is not as ubiquitous as the cell phone. Tens of millions of citizens opt into using technologies like Fitbit and Apple watches, health apps, journal apps (such as iPhone's built-in Notes App), apps for tracking menstrual cycles, ChatGPT, and smart cars, and those technologies record the most intimate, retrospective information about them. *See, e.g.*, William Gallagher, *Apple Watch Sets New US Record, now Owned by 30% of iPhone Users*, Apple Insider (Oct. 14, 2022), https://appleinsider.com/articles/22/10/14/apple-watch-sets-new-us-record-now-owned-by-30-of-iphone-users [https://perma.cc/DJ2P-LR7B] (100 million active users of Apple Watch in 2022); *Flo Health Inc. Company Update, March 2022*, Flo Health (Mar. 16, 2022), https://flo.health/newsroom/flo-company-update [https://perma.cc/N7Q6-V3UF] (220 million downloads of popular menstrual-cycle app); Krystal Hu, *ChatGPT sets record for fastest-growing user base - analyst note*, Reuters (Feb. 2, 2023), https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/ [https://perma.cc/R63F-EAPC] (100 million monthly users of ChatGPT within two months of launching).

Google alone has 1.5 billion users worldwide. *See* NYU Technology Law & Policy Clinic Amicus Brief at 5 n.4. Even if only one-third opt into Location History, that is a whopping 500 million people, many of whom are Americans. And millions more opt into

substantially identical location tracking through other technologies.[8] Far be it from me to tell hundreds of millions of Americans that they have waived their privacy rights with the State just because these invasive technologies are not fully automatic or because not *every single* user utilizes them.

Third, the gloss of an opt-in checkbox does not render the enabling of Location History collection "meaningful[ly]" voluntary.[9] *Carpenter*, 585 U.S. at 315. This one click

---

[8] While Location History is Google-specific, millions of Americans use substantially similar technologies offered by other companies. In *Carpenter*, the Court referred to the *total* number of cell phone service accounts in the United States, as opposed to the number of accounts with the specific wireless company that the defendant used. *Carpenter*, 585 U.S. at 300, 302. Thus, the correct analysis in assessing whether a technology is widely adopted and hence "indispensable to participation in modern society," *id.* at 315 (quotation omitted), is to consider the total number of users of substantially similar technologies.

[9] According to the majority, a user must (1) enable location sharing on their device; (2) enable the "Location Reporting" feature; (3) sign into Google; and (4) opt into the Location History setting. But the district court made no mention of, nor any findings of fact regarding, the enabling of location sharing or Location Reporting (the majority's requirements 1 and 2). *See Chatrie*, 590 F. Supp. 3d at 907–12. Rather, the district court concluded that users enable the Location History feature solely by opting into Location History and logging into their Google accounts.

Even if all four steps were required to enable Location History, the record indicates that these steps may be accomplished in the first few moments of setting up and using an Android device. Chatrie used a standard Android cell phone with Google's operating system. That type of phone comes out of the box with the location-sharing setting enabled *by default*, thus automatically satisfying requirement (1). Next, the record indicates that by enabling Location History, users can also automatically opt-in to Location Reporting. So, requirements (2) and (4) are not necessarily two separate steps; they can be completed with one click.

Likewise, one of the first steps in setting up an Android is to log into or create a Google account. Indeed, if users choose not to log into Google, they cannot use most of the Android's features such as downloading apps, music, and games; accessing Google (Continued)

does not meaningfully inform users that they are surrendering "a comprehensive dossier of [their] physical movements." *Id.*

Instead, the pop-up text that appears when Google prompts users to opt in explains only that Location History "[s]aves where you go with your devices," and that "[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com." *Chatrie*, 590 F. Supp. 3d at 911–12. Below that, the screen provides the options: "NO, THANKS" or a brightly highlighted "TURN ON." *Id.* at 912. It also presents a small expansion arrow, which, if tapped by the user, displays more information about Location History.[10] But a user does not need to click the expansion arrow to opt into Location History. They can just click "TURN ON." Through that click, Location History is enabled.

Maps; or syncing services like Calendar and Contacts. The district court found that Google repeatedly prompts its millions of Android users to opt-in to Location History both upon initial set-up and then "multiple times across multiple apps." *Id.* at 908–09 (cleaned up). For example, "Google may prompt the user to enable Location History first in Google Maps, then *again* when he or she opens Google Photos and Google Assistant for the first time." *Id.* at 909 (emphasis added). Thus, requirement (3) is also satisfied quickly and without reference to Location History.

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

The district court noted that this pop-up "did not detail . . . how frequently Google would record [a user's] location . . . ; the amount of data Location History collects (essentially all location information); that even if he 'stopped' location tracking it was only 'paused' . . . ; or, how precise Location History can be (i.e., down to twenty or so meters)." *Id.* at 936 (cleaned up). Nor did it inform users that Google would automatically and precisely track their location even when they were not doing anything on their phones, or that this tracking would occur across all devices on which they were logged in—not just those on which they opted in—even when they have deleted the respective Google app. *Id.* at 909–12 (quoting terms); *see id.* at 909 n.11, 913–14 & n.16 (discussing wide criticism of Google because its Location History opt-in and opt-out procedures were unclear to users); *cf. Jones*, 565 U.S. at 417 n.* (Sotomayor, J., concurring) ("[S]mart phone[] [owners] do not contemplate that these devices will be used to enable covert surveillance of their movements.").

I agree with the district court's conclusion that the warnings provided by Google are "limited and partially hidden" and that it is "plain that these 'descriptive texts' are less than pellucid." *Chatrie*, 590 F. Supp. 3d at 936. Simply put, the pop-up box lacked sufficient information for users to knowingly opt into Location History. Smartphone users are bombarded with opt-in buttons and terms of service in their daily phone use. Few actually read the terms, and, without reasonably clear descriptions, most users do not understand what they are approving. *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (pointing out that Americans are revealing intimate information during "mundane" tasks); *Research Shows Mobile Phone Users Do Not Understand What Data They Might Be Sharing*, Sci.

Daily (May 9, 2023), https://www.sciencedaily.com/releases/2023/05/230509122057.htm [https://perma.cc/54V5-Y49P] (discussing study that showed a substantial portion of users do not understand how phone and app tracking works).

Further, while the majority opinion argues that users can delete information, *see* Maj. Op. at 20, that is easier said than done. To delete their Location History, a user has "only one option": they must visit the proper website, locate their timeline, and delete their data. *Chatrie*, 590 F. Supp. 3d at 913. And the deletion of past Location History data will not turn off the collection of *additional* Location History data. As the district court indicated, the process of enabling, pausing, and deleting Location History is *not* transparent to users. *See id.* at 913–14, 936; *see also id.* at 913 (finding that Google falsely told users that pausing Location History will limit the functionality of Google services).

For instance, the district court quoted an internal email by a Google staffer who expressed their frustration that the Location History interface is "difficult enough that people won't figure . . . out" how to turn off the feature. *Id.* at 913. The district court determined that the sentiment in that email is "certainly not inconsistent with the record before the Court." *Id.* What's more, around the time Chatrie enabled the feature, Google faced criticism from members of Congress, the media, and Norway's Consumer Protection

Committee for the lack of transparency in how users enable or disable Location History. *See id.* at 909 n.11; *id.* at 913–14; *id.* at 913 n.16.[11]

The explosive growth of the usage of new technologies, such as smartphones, illustrates a certain level of comfort among the American populace in entrusting personal information to technology companies like Google. But that does not mean such trust extends to the State or that the American populace has ceded its reasonable expectation of privacy in that information. Americans might expect that companies provided with their information will, at most, barrage them with advertisements. The State, by contrast, holds a monopoly on licit violence and detainment. It is a grave misjudgment to conflate an individual's limited disclosure to Google with an open invitation to the State. *See Jones*, 565 U.S. at 418 (Sotomayor, J., concurring) ("I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."); *Smith*, 442 U.S. at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those

[11] The majority opinion argues that the evidence is "nonexistent" that pausing or deleting Location History is easier said than done. Maj. Op. at 35 n.30. But the majority provides no evidence of its own that pausing and deleting Location History is a reasonable process for users, beyond stating conclusively that users can figure it out. *Id.* at 20–21, 35 n.30. And to the contrary, criticism from the news media, congressional members, a consumer-protection group, and Google staffers themselves regarding the difficulty of pausing or deleting Location History certainly constitutes evidence of the same. Moreover, though the district court did not conduct fact-finding on this issue, it did conclude that such criticisms appeared consistent with the record and that Google's warnings were "less than pellucid." *Chatrie*, 590 F. Supp. 3d at 936, 913.

who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").

As noted, *Carpenter* endorses a normative understanding of modern technology and with it a normative understanding of voluntariness. *See Carpenter*, 585 U.S. at 315 (concluding that "*in no meaningful sense* does the [cell phone] user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements" (emphasis added) (cleaned up)). Although bank records and the dialing of phone numbers are similarly central to participation in modern society, the Court in *Carpenter* opted to treat the conveyance of CSLI as uniquely involuntary. This demonstrates a recognition that modern technology, particularly that which tracks an individual's location, warrants heightened privacy requirements.

In sum, even if voluntariness might be considered as a factor in the *Carpenter* test, the conveyance of Location History data to third parties is not meaningfully voluntary. And even assuming arguendo that it is marginally more voluntary than the conveyance of CSLI was in *Carpenter*, the balance of the *Carpenter* factors nonetheless strongly supports the conclusion that the geofence intrusion constituted a search.

* * *

Because the balance of the *Carpenter* factors shows that Location History is qualitatively different from the records that police could traditionally obtain without a warrant, Chatrie had a reasonable expectation of privacy in his Location History data, and the government conducted a search by accessing it. In the context of this novel technology,

the third-party doctrine is wholly inadequate to defeat that reasonable expectation. While geofence intrusions may be a boon to law enforcement, they still require a warrant.

B.

My friends in the majority rest their contrary holding on Section III(B) of *Carpenter*, in which the Court rebutted the government's insistence that *Smith* and *Miller* should resolve the case. In so doing, the majority decision holds that the proper analysis under *Carpenter* is a direct analogy to the third-party doctrine established by *Smith* and *Miller*. *See* Maj. Op. at 22 ("The third-party doctrine . . . squarely governs this case.").

But *Carpenter* affirmatively *rejected* a "straightforward application" of *Smith* and *Miller*, establishing that analogizing the third-party cases to "qualitatively different" records like CSLI and Location History is misguided. *Carpenter*, 585 U.S. at 309, 314; *see id.* at 314 ("The Government . . . is not asking for a straightforward application of the third-party doctrine, but instead *a significant extension of it* to a distinct category of information. . . . In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI." (emphasis added)); *see also id.* at 313 (rejecting Government's argument that "cell-site records are fair game because they are 'business records' created and maintained by the wireless carriers").

Thus, *Smith* and *Miller* do not control here because the *Carpenter* Court rejected a simplistic analogy to those cases when dealing with advanced digital surveillance. Further, even if such an analogy were proper, the nature of the records collected here is incomparable to those in third-party cases like *Smith* and *Miller* so the application of the

third-party doctrine fails. Indeed, the third-party doctrine has two requirements: first, the nature of the documents sought by police must be unrevealing business records like those in *Smith* and *Miller*, and second, the conveyance to the third-party company must be meaningfully voluntary. As *Carpenter* emphasized, "*Smith* and *Miller* . . . did not rely solely on the act of sharing. Instead, [those decisions] considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'" *Id.* at 314 (quoting *Miller*, 425 U.S. at 442). So even if the conveyance of Location History was voluntary, the *Carpenter* Court repeatedly stressed that the nature of location data derived from a smart phone—such as the CSLI data in *Carpenter*, or the Location History data here—is simply incomparable to that sought in *Smith* and *Miller*.

In analyzing the "nature of the particular documents sought" in this case, the majority decision instead concludes that the geofence intrusion here was "far less revealing than that obtained in *Jones*, *Carpenter*, or *Beautiful Struggle* and more like the short-term public movements in *Knotts*." Maj. Op. at 19–20.

But that's an improper comparison. Instead, the proper comparison in applying the *third-party doctrine* would be to the bank documents and pen register in the *third-party cases*, *Smith* and *Miller*—not to the public-surveillance cases cited in the majority decision. *E.g.*, *Carpenter*, 585 U.S. at 313–14 (comparing CSLI to the documents in *Smith* and *Miller*); *id.* at 306 (distinguishing public surveillance and third-party doctrine cases); *Smith*, 442 U.S. at 741–43 (addressing nature of records); *Miller*, 425 U.S. at 440–43 (same). The

majority opinion's failure to grapple with *Smith* and *Miller*, while insisting that "[t]he third-party doctrine . . . squarely governs this case," Maj. Op. at 22, is telling.

As discussed above, the *Carpenter* Court took great pains to emphasize that the nature of technology like CSLI is "unique," "an entirely different species," "a qualitatively different category" of information, and data that represents a "seismic shift[]" in technology as compared to the phone numbers dialed and bank records in *Smith* and *Miller*. *Carpenter*, 585 U.S. at 309, 313, 318. And as my analysis has shown, the first four *Carpenter* factors demonstrate that the "nature" of Location History, like CSLI, differs by orders of magnitude from the records at issue in the third-party cases.

Beyond that, *Carpenter* rejected the application of the third-party doctrine by explaining that the third-party cases relied on the unrevealing nature of the documents sought. *Id.* at 313–14. For instance, *Carpenter* explained, the *Smith* Court stressed that the phone numbers lacked any content or "identifying information" in holding there was no reasonable expectation of privacy. *Id.* at 314 (cleaned up); *see also Smith*, 442 U.S. at 741.

By contrast, Location History, like the CSLI in *Carpenter*, reveals that information. Thus, "[s]uch a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Carpenter*, 585 U.S. at 315. *Carpenter* emphasized that unless courts recognize this difference, they will "fail[] to appreciate that there are no comparable limitations on the revealing nature of CSLI." *Id.* at 314. So too here. *Carpenter* hence rejected the view that the nature of personal-location data matches that of traditional bank or phone records, urging courts to consider the context of *Smith* and *Miller*'s analyses.

Thus, even if the conveyance of Location History was voluntary, the first prong of the third-party-doctrine test—the nature of the records conveyed—is nowhere near satisfied and the application of the doctrine here fails. Accordingly, *Carpenter* compels the conclusion that the police intrusion into Chatrie's Location History data constituted a Fourth Amendment search.[12]

III.

Before concluding, I respond to what the majority opinion structures as a lengthy separate opinion that responds to my dissent, Maj. Op. at 23–35.

Extrajudicially, the majority's separate opinion claims that *Carpenter*'s factor-based test was "concocted" from thin air. *Id.* at 24. Instead, the majority opinion believes that (1) *Carpenter* should be read narrowly to apply only the "established" privacy principles pronounced in *Jones*, *id.* at 25; (2) employing a factor-based test would "abandon[]" all pre-*Carpenter* case law, *id.* at 23, 31; and (3) despite the *Carpenter* Court's warnings about applying old tests to new technologies, the third-party doctrine can nonetheless definitively settle this case, *id.* at 31–35. All three beliefs are unsound.

[12] The government did obtain a warrant in this case. But I agree with the lower court that the warrant here was so lacking in particularity and probable cause that it was invalid. *Chatrie*, 590 F. Supp. 3d at 927. And the good-faith exception to the warrant requirement does not apply because the warrant lacked any indicia of probable cause. The government's proposed justification—that the robber used a cell phone and a cell phone *could* have Google Location History turned on—is extremely broad. Also, the government did not limit the scope of the warrant to an area reasonably related to the bank robbery. Accordingly, a reasonable officer could not have relied on the warrant in good faith. I would thus grant Chatrie's Motion to Suppress the evidence that resulted from the geofence search.

A. *Carpenter* Established a Multifactor Analysis

In an attempt to restructure the Supreme Court's holding in *Carpenter*, the majority folds that decision into *Jones*, saying that *Jones* had established certain rules regarding the privacy implications of digital technology and first identified the relevant factors, and that *Carpenter* merely applied those rules and factors. *See id.* at 24 (claiming that *Carpenter* simply "appl[ied] the principles announced in the location-tracking cases"); *id.* at 25 (asserting that *Jones* considered unique qualities of GPS technology like that it is "detailed, encyclopedic, and effortlessly compiled," and *Carpenter* merely "applied" those "established principles" to CSLI). So, with that, the majority declares that *Carpenter* accomplished nothing new.

But that's wrong. As we acknowledged in *Beautiful Struggle*, *Jones* "was ultimately decided on trespass principles." *Beautiful Struggle*, 2 F.4th at 341. Indeed, the *Jones* majority analyzed only the trespass doctrine, expressly declining to consider the privacy implications of a GPS intrusion under *Katz*. *Jones*, 565 U.S. at 406–07. Significantly, it was the *concurring justices* in *Jones* who pointed out the unique attributes of GPS technology and argued that the *Katz* reasonable-expectation-of-privacy test could have decided the case.

Specifically, in his concurring opinion, Justice Alito, joined by three other Justices, argued that the long-term GPS intrusion in *Jones* violated *Katz* because society did not historically expect police to conduct such prolonged surveillance on public streets due to practical limitations like cost. *Id.* at 429–30 (Alito, J., concurring in judgment). And it was Justice Sotomayor who, writing alone, discussed several unique attributes of GPS—that it

is precise, comprehensive, intimate, retrospective, and cheap—and argued that those attributes implicate the *Katz* analysis for even short-term GPS surveillance. *Id.* at 415–16 (Sotomayor, J., concurring). So, it was the concurrences in *Jones*—and particularly that of Justice Sotomayor, writing alone—that recognized the unprecedented power of modern location-tracking technology and argued for the need to adjust Fourth Amendment protections to maintain traditional privacy expectations against such technologies. But, prior to *Carpenter*, that view was not binding precedent.

Carpenter hence broke new ground: it placed the principles proposed in the *Jones* concurrences (the four-justice opinion of Justice Alito coupled with the concurring opinion of Justice Sotomayor) into a majority opinion and articulated how location data obtained from a cell phone is different from traditional modes of surveillance. As explained, the *Carpenter* majority derived most of its factor-based test from Justice Sotomayor's lone concurrence in *Jones*. In addition, *Carpenter* marked the first time that the Court in a majority opinion recognized a privacy interest in the "whole of [a person's] physical movements," and it weighed those factors to analyze that interest. *Carpenter*, 585 U.S. at 310. So, *Carpenter* marked a new era of Fourth Amendment jurisprudence even as it built on the cases that came before it, setting forth how we must think about the Fourth Amendment in the context of modern technology.

Thus, the majority opinion's claim that *Carpenter* merely "applied established principles" is wrong. Maj. Op. at 25. And to confirm that, we need to look no further than the *Carpenter* opinion itself, which explicitly stated that its decision "d[id] not fit neatly under existing precedents." *Carpenter*, 585 U.S. at 306. That statement alone should end

this discussion but in the interest of completeness, I will respectfully address the remainder of the majority opinion's complaints about *Carpenter*'s multifactor analysis.

The majority opinion scoffs that the factor-based test does not exist. Maj. Op. at 23–26. But this dissent's analysis of the test comes directly from *Carpenter*'s text, in which the Supreme Court took great pains to make clear that the third-party doctrine cannot extend to novel technologies like CSLI that have the qualities the Court identified. The Court's efforts were apparently in vain, however, because the majority opinion continues to "mechanically apply[] the third-party doctrine" in defiance of the Supreme Court's repeated and express commands not to do so. *Carpenter*, 585 U.S. at 314.

Remarkably, while alleging that this dissenting opinion's analysis lacks any basis in *Carpenter*, the majority opinion simultaneously complains that this dissent quotes *Carpenter too much*—particularly the Court's language stressing the distinct nature of CSLI and directing courts to move away from past doctrine when analyzing such technology. *See* Maj. Op. at 24 & n.21. That's just poppycock. Instead of engaging with the substance of the Supreme Court's quoted language that forms most of *Carpenter*'s analysis, the majority answers by essentially saying we should ignore that language.

Still further, the majority opinion posits that the "'factors' identified by [this] dissent . . . were not factors at all" but were instead "attributes" of CSLI that "implicated the privacy interest recognized by the concurring Justices in *Jones*." *Id.* at 25. That is a distinction without a difference. In other words, although the majority quibbles about how to characterize the Court's analysis (factors vs. attributes), it recognizes that those factors (or attributes) are derived directly from *Carpenter*'s text. For example, the majority agrees

that the CSLI in *Carpenter* implicated the reasonable-expectation-of-privacy test because the CSLI had "immense capabilities": that is, it "provided a '*comprehensive* record' of [the defendant's] movements, which revealed *intimate* details of his life . . . . And the *retrospective* nature of CSLI and the *ease* by which it could be accessed only augmented these privacy concerns, for no comparable record of a person's movements was available to law enforcement in a pre-digital age." *Id.* (emphases added) (quoting *Carpenter*, 585 U.S. at 309). Because CSLI had each of those qualities, the majority opinion concedes, "CSLI warranted Fourth Amendment protection." *Id.*

In so conceding, the majority opinion applies the exact factors I recognize in this dissent, pointing out that, post-*Carpenter*, we consider comprehensiveness, intimacy, retrospectivity, and ease when determining whether a digital intrusion violates the Fourth Amendment. So, whether we call the qualities that we weigh "attributes" or "factors" is immaterial. As explained, *supra* at 48–49, the *Carpenter* Court did not expressly state that it created a factor-based test; it identified the qualities of CSLI that informed its holding. The legal community—including three of the dissenting Justices on the *Carpenter* Court, *see Carpenter*, 585 U.S. at 340 (Kennedy, J., joined by Thomas and Alito, JJ., dissenting)—has concluded that those qualities created a factor-based test.

So the factor-based test is certainly not the "creative[]" project of this dissenting opinion, as the majority suggests. Maj. Op. at 32 n.27; *accord id.* at 24 (characterizing this dissent's "pronouncements" as "bold" and its "framework" as "novel"); *id.* (criticizing this dissent for "combin[ing] . . . ingredients" from *Carpenter* to "create[] a new inquiry from scratch" in order to—"*voila!*"—find that a search occurred); *id.* at 35 (arguing that this

dissent's test is "novel" and "unwieldy"). Instead, it represents the scholarly consensus that *Carpenter* diverged from existing precedent and created a new, multifactor analysis. In addition to the leading authorities this dissenting opinion has already cited, *see supra* at 49–50 (first citing Ohm, *supra*, at 363, 369; then citing Freiwald & Smith, *supra*, at 219; and then citing *Tokson*, *The Aftermath of* Carpenter, *supra*, at 1830), numerous other scholars and authorities to have considered the issue have concluded the same, *see*, *e.g.*, Sherwin Nam, *Bend and Snap: Adding Flexibility to the* Carpenter *Inquiry*, 54 Colum. J.L. & Soc. Probs. 131, 132 (2020) (stating that *Carpenter* "broke new ground in the constitutional right to privacy in electronic data" and employed a "five-factor" test); Helen Winters, *An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants*, 107 Minn. L. Rev. 1369, 1381, 1390 (2023) (stating *Carpenter* "marked a new period of Fourth Amendment jurisprudence" and described "several factors relevant to its decision"); Antony Barone Kolenc, *"23 and Plea": Limiting Police Use of Genealogy Sites After* Carpenter v. United States, 122 W. Va. L. Rev. 53, 71–72 (2019) (concluding that *Carpenter* "alter[ed] Fourth Amendment law" by recognizing a privacy interest in the "whole of a person's physical movements," and "balanced five factors" to analyze that interest); Allie Schiele, *Learning from Leaders: Using* Carpenter *to Prohibit Law Enforcement Use of Mass Aerial Surveillance*, 91 Geo. Wash. L. Rev. Arguendo 14, 17–18 (2023) (pointing out "*Carpenter*'s focus on five central factors"); Nicole Mo, *If Wheels Could Talk: Fourth Amendment Protections Against Police Access to Automobile Data*, 98 N.Y.U. L. Rev. 2232, 2251 (2023) (recognizing factors); Luiza M. Leão, *A Unified Theory of Knowing Exposure: Reconciling* Katz *and* Carpenter,

97 N.Y.U. L. Rev. 1669, 1684 (2022) (same); Matthew E. Cavanaugh, *Somebody's Tracking Me: Applying Use Restrictions to Facial Recognition Tracking*, 105 Minn. L. Rev. 2443, 2468 (2021) (same).

Finally, the majority opinion laments that the multifactor analysis only works if *Carpenter* created a test "from scratch." *Id.* at 24. But that is far from the case.

Rather, *Carpenter* articulated the factors as a way to analyze whether an individual has a reasonable privacy expectation in their digital location data. So, the Court applied the long-standing *Katz* standard, but it adapted the *Katz* analysis for digital data like CSLI to preserve privacy protections against encroaching technologies—which, as *Carpenter* explained, the Court has done throughout its Fourth Amendment jurisprudence. *Carpenter*, 585 U.S. at 304–05 (noting that the Court "ha[s] kept . . . Founding-era understandings [of privacy] in mind when applying the Fourth Amendment to innovations in surveillance tools" and citing cases in which the Court "rejected . . . a 'mechanical interpretation' of the Fourth Amendment" for novel surveillance tools (citations omitted)).

Thus, *Carpenter*'s analysis *began* by providing this context and explaining the Court's enduring understanding that expansive technologies require heightened protections. *Id.* at 304–05. In so doing, the Court situated the remainder of its analysis within that context. And the Court repeated those sentiments throughout the opinion. The majority opinion ignores these critical aspects of *Carpenter*.

Carpenter also acknowledged the Court's existing third-party-doctrine precedent but explained that the *Carpenter* factors render the "nature" of CSLI markedly different from the nature of the documents in the third-party cases. *Id.* at 308–10. In addition, the

Court's opinion incorporated ideas about technology and privacy from past cases like *Kyllo*, *Riley*, and the *Jones* concurrences. *E.g.*, *id.* at 310–13. For these reasons, *Carpenter*'s multifactor analysis was "informed" by case law and adapted for a new era. *Id.* at 305.

But not to be deterred even in a world ever transfigured by technology, the majority opinion apparently wants to scold the *Carpenter* Court for stepping beyond the shadows of *Knotts*, *Smith*, and *Miller* when faced with surveillance technology that is not only different in degree, but different in kind. I must disagree, because the Supreme Court's analysis in *Carpenter* aptly reflects the traditional evolution of law. That is, the Supreme Court wisely moved beyond its decades-old precedent to reiterate that it is not required to robotically copy and paste precedent when dealing with novel issues arising from changing technology.

Nonetheless, the majority opinion contends that the Supreme Court could not have possibly "abandoned" *Knotts*, *Jones*, *Smith*, and *Miller* in the face of new technology. Maj. Op. at 23, 31. I agree that the Supreme Court did no such thing. That's because *Jones* was resolved under trespass principles; *Knotts* involved surveillance of a suspect during one trip on public roads using what *Carpenter* called a "rudimentary" beeper, *Carpenter*, 585 U.S. at 306; and *Smith* and *Miller* involved police obtaining bank records and dialed phone numbers, which *Carpenter* emphasized were "a world" apart from data like CSLI and Location History, *id.* at 314.

Thus, *Carpenter* did not "abandon" *Knotts*, *Smith*, and *Miller*—instead, it explained that they do not neatly apply to technologies like CSLI and Location History. In so holding,

Carpenter acknowledged a simple truth: the digital age does not strip us of our Constitutional protections.

And this principle is not what the majority calls a radical departure because it is no more revolutionary than the novel acknowledgments in *Katz* that the "Fourth Amendment protects people, not places," or in *Riley* that our cell phones are not merely external attachments, but intimate extensions of our private lives. *Id.* at 304–05 (first quoting *Katz*, 389 U.S. at 351; and then citing *Riley*, 573 U.S. at 393). At bottom, *Carpenter* binds this Court and we must follow it.

B. The *Complete* Third-Party Analysis, Intimacy, and Standing

The majority opinion also complains that the Location History intrusion at bar did not reveal information as intimate as that in *Carpenter* and *Beautiful Struggle*, and that the use of Location History is voluntary. Maj. Op. at 26–35. Relatedly, the majority opinion reiterates that even if the intrusion entered private spaces, Chatrie lacked Fourth Amendment standing to challenge it because, as far as we know, it did not enter *his* protected spaces.

In other words, the majority opinion emphasizes two of *Carpenter*'s five factors (intimacy and voluntariness)—but it ignores the remaining three factors (comprehensiveness, in terms of both depth and breadth; retrospectivity; and efficiency), likely because they weigh indisputably in Chatrie's favor. It likewise ignores the other prong of the third-party doctrine, the nature of the documents sought, which similarly forecloses the use of that doctrine. I address the third-party doctrine before discussing intimacy.

1.

First, take the third-party doctrine. As the majority makes clear, it believes that the use of Location History is meaningfully voluntary because the average user should know from Google's popups, which the district court called "limited and partially hidden" and "less than pellucid," that Google will infinitely track the user's Location History data. *Chatrie*, 590 F. Supp. 3d at 936. But nothing in the majority opinion's lengthy response to my dissent addresses the first requirement of the third-party doctrine—the nature of the documents collected. The third-party doctrine has *two* requirements. First, the "nature of the particular documents sought" must be akin to the unrevealing business records (the phone numbers dialed and bank records) at issue in *Smith* and *Miller*. *Carpenter*, 585 U.S. at 314 (quoting *Miller*, 425 U.S. at 442). Second, those records must be voluntarily conveyed to the third-party business. *Id.*

As discussed above, the majority opinion's third-party-doctrine analysis is flawed because it wrongly compares the "nature of the documents" at issue here to the nature of the surveillance in *Knotts* (outdoor beeper surveillance), *Jones* (outdoor GPS-tracker surveillance), and *Beautiful Struggle* (outdoor aerial surveillance), even though those cases did not involve the conveyance of records to third parties. Rather, to properly apply the *third-party doctrine*, we must compare the nature of the documents in this case to those in the *third-party doctrine* cases, i.e., *Smith* and *Miller*. By instead selecting inapt comparators, the majority opinion crafts a Frankensteinian analysis that lacks a basis in precedent or logic. And while it insists that the third-party doctrine "squarely" applies here,

Maj. Op. at 22, the majority opinion ignores comparisons to the documents in the third-party doctrine's seminal cases.

As *Carpenter* stressed, the nature of CSLI and Location History data today is miles apart from that of phone and bank records in the 1980s. Because the first prong of the third-party doctrine fails, so too does the application of the doctrine to this case. So, a straightforward application of the doctrine mandates the conclusion that a Fourth Amendment search occurred here.

2.

The majority opinion next relies on *Beautiful Struggle*, in which this Court held that Baltimore's weeks-long public aerial surveillance constituted a Fourth Amendment search, to conclude that the two-hour intrusion at bar could not gather data that was sufficiently intimate so as to implicate the Fourth Amendment. Thus, the majority opinion argues that, unlike the longer intrusion in *Beautiful Struggle*, the intrusion here was too short to reveal intimate information and thus was not a search. Maj. Op. at 26–29. In so arguing, the majority opinion expounds on its assertion that Chatrie lacked standing to challenge the intrusion if it did not enter his private spaces. *Id.* at 30–31. These arguments relate to the majority opinion's final objection that *Beautiful Struggle* did not recognize any factor-based inquiry from *Carpenter*, and thus, the majority opinion reasons, one does not exist. *Id.* at 25–26.

These arguments fall flat. As I explain, the intimacy discussion in *Beautiful Struggle* does not foreclose a finding of intimacy here because that case involved technology that was only capable of surveillance of public movements. And the majority opinion

misrepresents that *Beautiful Struggle* did not recognize any factor-based test from *Carpenter* because that opinion expressly applied the *Carpenter* factors.

As a threshold matter, however, the majority opinion's argument is unclear. It claims that *Carpenter* did not apply any multifactor analysis, and that *Beautiful Struggle* instead established its own test: a search occurs when police "use technology to monitor [an individual's] long-term movements, but not when they glimpse only his short-term movements." *Id.* at 26. In other words, the majority opinion remarkably proposes that the Fourth Amendment only considers whether an intrusion using modern technology was long or short. But then the majority opinion informs us that "Location History has capabilities much like GPS data and CSLI," *id.* at 29, seemingly referring to the *Carpenter* factors, which should be irrelevant to the supposedly sole question of an intrusion's length. And, as noted, in another portion of its response to my dissent, the majority opinion tellingly applies the *Carpenter* factors itself. *Id.* at 25. In essence, the majority opinion flip-flops to reach a desired outcome. I nonetheless respond to its arguments.

a.

The majority opinion's argument that *Beautiful Struggle* forecloses a finding of intimacy for all relatively short intrusions misconstrues the opinion and stretches it further than the opinion can bear. To explain why *Beautiful Struggle* is not on point, I begin with some background.

In *Beautiful Struggle*, the Court considered Baltimore's aerial-surveillance program, which monitored only public spaces and stored that data for forty-five days. The aerial surveillance generally gathered hours-long chunks of surveillance during the day, and only

showed individuals as anonymous, blurry pixels. *Beautiful Struggle*, 2 F.4th at 334, 340. As a result, the government had to decipher individuals' identities from several pieces of captured data. *Id.* at 334.

The key distinction between Baltimore's program and CSLI or Location History is that it strictly captured *public* movements. The Supreme Court has long held that individuals have a diminished privacy expectation in public spaces. *See Katz*, 389 U.S. at 351. As part of this diminished privacy expectation, the Court recognized in *Knotts* that beeper surveillance of one public trip did not implicate the Fourth Amendment. *Knotts*, 460 U.S. at 285. Crucial to the *Knotts* Court's holding, however, was the beeper's rudimentary capabilities that merely augmented human senses, such that the surveillance mirrored that of a passerby watching the defendant on the street. *See Carpenter*, 585 U.S. at 306–07.

So, in analyzing the public surveillance in *Beautiful Struggle*, this Court had to begin with the tenet that one has a diminished privacy expectation in public, then to ask whether the surveillance was so invasive as to breach that diminished privacy expectation. And, if the intrusion was to be considered a Fourth Amendment search, it would have to be more invasive than that in *Knotts*. This is where the duration of the intrusion becomes relevant. The district court in *Beautiful Struggle* had determined that Baltimore's aerial intrusion was not a search because the program captured only chunks of *public* movements. *Leaders of A Beautiful Struggle v. Balt. Police Dep't*, 456 F. Supp. 3d 699, 713–14 (D. Md. 2020) (reasoning that the intrusion could not reveal details inside of private spaces).

But this Court reversed, holding that the forty-five-day length of the public aerial surveillance implicated the *Carpenter* factors. That is, we held that because the government gathered chunks of public aerial footage daily for weeks, the cumulative data was "detailed, encyclopedic," "intimate," and "retrospective," and broadly comprehensive because it "recorded *everyone's* movements." *Beautiful Struggle*, 2 F.4th at 341–42 (cleaned up); *see id.* at 345 (explaining that people reasonably expect to be seen for a short period in public, but they do not expect longer public intrusions). And we emphasized that the weeks-long duration of the intrusion permitted deductions by police that revealed "intimate" information about those surveilled. *Id.* at 342. For all those reasons, we determined that Baltimore's relatively lengthy public surveillance "transcends mere augmentation of ordinary police capabilities" and hence triggered Fourth Amendment protections. *Id.* at 345.

So, while this Court in *Beautiful Struggle* did distinguish between a short- and long-term search, that was because the search at issue in that case covered strictly public areas. *Id.* at 341. Contrary to the majority opinion's assertions, the distinction that we drew in *Beautiful Struggle* regarding the length of the search was rooted in the factors that *Carpenter* identified. Its solely public sweep notwithstanding, the longer aerial intrusion was a search *because* it satisfied the *Carpenter* factors and thus violated the surveilled individuals' reasonable privacy expectations. *Id.* at 341–42, 346 (applying factors and concluding the intrusion was a search). If in *Beautiful Struggle* we believed those factors were irrelevant, as the majority opinion now presses, then we would have simply distinguished *Knotts* without saying more.

Technology that allows only for augmented public surveillance, however, is fundamentally different from technology that has the capacity to surveil private spaces, like CSLI and Location History.[13] This is nothing new: the Supreme Court has long drawn a line between public and private spaces—concluding that using a beeper to track a vehicle for one trip on a public road is not a search, but monitoring a device within a constitutionally protected space is subject to Fourth Amendment constraints, even if the monitoring was brief or revealed nothing of value. *Compare Karo*, 468 U.S. at 714–15, *with Kyllo*, 533 U.S. at 34. Unlike in public, individuals do not have a diminished privacy expectation in private spaces. Accordingly, where a police intrusion can enter private spaces, the short-versus-long-term distinction holds much less weight.

Relatedly, the fact that Location History can perfectly surveil private spaces implicates one's reasonable privacy expectation because it exceeds historical expectations of police capabilities. In *Beautiful Struggle*, the Court reasoned that a short aerial intrusion only augmented what police could traditionally capture by tailing suspects. Only public surveillance for a longer duration amounted to "attaching an ankle monitor" to those surveilled, *Beautiful Struggle*, 2 F.4th at 341 (cleaned up), capturing information that police traditionally could not gather "without technology," *id.* So there, only the longer intrusion violated privacy expectations and became a search. But here, even two hours of a boundless

[13] The majority opinion claims that we cannot even consider the differences in the capacities of the technologies at issue in *Beautiful Struggle* and the present case because the Location History data here only captured public movements. Maj. Op. at 31. But, as explained above, whether a person has a reasonable expectation of privacy in certain forms of data depends on the *capabilities* of that data. *Supra*, at 58–60.

Location History intrusion is akin to "attaching an ankle monitor" on the surveilled, capturing information inside private spaces that were historically closed to prying police eyes. That intrusion thus exceeds mere augmentation of human capabilities and becomes a search, even when the duration is short. *See id.* at 341, 343, 345 (emphasizing that the analysis turns on historical police capabilities).

Similarly, we also reasoned in *Beautiful Struggle* that it would take longer for police to deduce intimate information about individuals whom they only follow on discrete public trips like that in *Knotts*, meaning that the duration of surveillance in the public sphere is a key component of the intimacy factor. *Id.* at 342–43. But an intrusion that provides near-perfect surveillance in *private* spaces, like with Location History data, much more quickly reveals one's "familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). So, again, the short-term and long-term distinction is less relevant outside of the public-surveillance context.

In sum, the majority opinion errs in contending that, following *Beautiful Struggle*, the only Fourth Amendment question before us is whether an intrusion was long or short. As our analysis in *Beautiful Struggle* demonstrated, we must ask whether an intrusion satisfied the *Carpenter* factors. While the length of the intrusion in *Beautiful Struggle* made clear that it did, a shorter intrusion into nonpublic spaces could satisfy the *Carpenter* factors as well—as it did here.

Next, the majority opinion argues that the geofence intrusion did not reveal intimate information because the two-hour window could have only revealed innocuous activities in private spaces, as opposed to scandalous or particularly sensitive activities. Maj. Op. at

28–29. It acknowledges that the geofence indeed could have captured users "seeing a friend for coffee, touring a housing upgrade, . . . buying a couch off of Facebook marketplace," or inquiring into medical services. *Id.* at 28. But because such innocuous activities would not reveal individuals' "habits, routines, and associations," the majority opinion argues, the intrusion was not sufficiently intimate to become a search. *Id.* at 28–29.

The majority opinion wrongly defines intimacy. *Beautiful Struggle* indeed held that surveillance that reveals one's "habits and patterns" is intimate. *Beautiful Struggle*, 2 F.4th at 343. But, contrary to the majority opinion's assertion, that is not the only information that is intimate for purposes of the Fourth Amendment reasonable-expectation-of-privacy test. Indeed, *Carpenter* made no mention of personal habits or patterns in its intimacy analysis. *Carpenter* instead held that an "intimate window" into a person's life is one that reveals "his 'familial, political, professional, religious, and sexual associations.'" *Carpenter*, 585 U.S. at 311 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). The sheer breadth of that list of associations—which the Court held contains the sacred "privacies of life" in which one maintains a reasonable privacy expectation, *id.* (quoting *Riley*, 573 U.S. at 403)—is telling. Of course, this Court's decision in *Beautiful Struggle* could not limit the reach of *Carpenter*; nor did it claim to do so. Instead, while habits and patterns relevant in *Beautiful Struggle* are indeed a *form* of intimacy, the litany of associations that *Carpenter* recognized are likewise intimate.

Because people have a reduced privacy expectation in public, it made sense that the public surveillance in *Beautiful Struggle* would only violate their privacy expectation when the surveillance was so invasive that it permitted deductions about their "habits and

patterns," from which police could decipher personal associations, which often manifest in non-public spaces. Habits and patterns are intimate precisely because they reveal the associations recognized in *Carpenter*. But when police can monitor individuals' precise movements in private spaces, the information revealed is much more intimate and likely to reveal one's familial, political, professional, religious, and sexual associations without the need for pattern-based deductions. Under the Fourth Amendment, Americans have a heightened privacy expectation from such intrusions.

The majority opinion's argument that innocuous information is not intimate is likewise unavailing. Two hours of innocuous activities in a busy urban area could certainly reveal the targets' associations. The Fourth Amendment has never incorporated a scandal barometer for information that constitutes the "privacies of life." *Id.* at 311.

Simply put, the majority opinion enacts a sweeping new rule: when it comes to data like Location History, police are only required to obtain warrants for longer intrusions—without any regard for the advancing capabilities of the surveillance technologies that police may use or the revealing nature of the data that the police may access. This blanket rule has no basis in *Carpenter*, which expressly declined to address whether a specific duration was necessary to implicate Fourth Amendment protections. Nor could this blanket rule find a basis in *Beautiful Struggle*, which addressed only police surveillance that captured blurry public movements.

b.

In the majority opinion's final attempt to argue that the intrusion here was not a search, the majority reiterates its argument that Chatrie had no standing to challenge the

intrusion if it did not enter his own private spaces. *See* Maj. Op. at 19 n.17, 30–31, 31 n.26. Because the majority opinion merely repeats itself without engaging with my response, *supra* at 58–60, I will not rehash this issue.

c.

Of note, the majority opinion focuses on intimacy and voluntariness in its lengthy response to this dissent. But intimacy is only one of the factors to which the Court looked in *Carpenter*. And even if the shorter duration of the intrusion in this case leads the intimacy factor to weigh less strongly in favor of deciding that the Fourth Amendment applies, it far from tips the scale given the immense weight of the comprehensiveness (in breadth and depth), efficiency, and retrospectivity of Location History. The majority opinion does not dispute that these factors apply to Location History.

As a self-provided example of "eviscerat[ing] basic and longstanding Fourth Amendment principles," Maj. Op. at 31 n.26, the majority opinion utterly fails to address the geofence's stark similarities to the reviled general warrants that the Fourth Amendment was intended to bar—similarities that will only increase given the majority opinion's elimination of the warrant requirement altogether. *See supra* at 62. At the very least, these historical similarities demand heightened caution here, not the majority opinion's rigid application of the third-party doctrine.

3.

Our Supreme Court decided *Carpenter* on the principle that applications of the Fourth Amendment must evolve in step with technology to ensure that our constitutional protections are not rendered meaningless by new means of government intrusion. Rather

than clinging to policy preferences for pre-*Carpenter* precedent, the Supreme Court in *Carpenter* directed courts to move past such basic analyses when considering unprecedented surveillance technology like CSLI.

It is our duty to apply *Carpenter* honestly and diligently. We should not and cannot sidestep the primary impact of a Supreme Court opinion to apply earlier decisions that are inapplicable, and simply put, more to our own liking. To do so would undercut *Carpenter* and thus, undermine our duty to faithfully guard Constitutional protections.

IV.

As a consequence of today's majority decision, significant concerns arise regarding the privacy rights of all Americans. That's why Justice Sotomayor's warning in *Jones* applies here with equal relevance—rejecting the warrant requirement for technology as cheap, readily accessible, and unprecedentedly powerful as a geofence intrusion is akin to inviting governmental abuse. *See Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

Ironically, court decisions like this one could also hinder legitimate law enforcement efforts. Shortly after oral arguments in this case, Google—apparently predicting the majority opinion's flawed reading of *Carpenter*—shut down the technology that permits geofence intrusions,[14] thereby reducing the potential for legitimate investigatory uses of this innovative technology, even with a warrant.

[14] *E.g.*, Cyrus Farivar & Thomas Brewster, *Google Just Killed Warrants That Give Police Access to Location Data*, Forbes (Dec. 14, 2023), https://www.forbes.com/sites/cyrusfarivar/2023/12/14/google-just-killed-geofence-warrants-police-location-data/ [https://perma.cc/27JX-ANVC].

Another consequence of today's decision is that it could "alter the relationship between citizen and government in a way that is inimical to democratic society." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (cleaned up). This is because citizens may feel inhibited from exercising their associational and expressive freedoms, such as the right to peacefully protest and the ability of journalists to gather information confidentially and effectively, knowing "that the Government may be watching" them. *Id.*; *see* Reporters Committee for Freedom of the Press Amicus Brief at 7–8 (noting the CIA's track record of "follow[ing] newsmen . . . in order to identify their sources" (citation omitted)); *Smith*, 442 U.S. at 751 (Marshall, J., dissenting) ("The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide."); *see* NYU Technology Law & Policy Clinic Amicus Brief at 25 (noting that "[f]orced disclosure of membership can chill association, even if there is no disclosure to the general public"); *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2388 (2021) (holding that disclosure requirements risk chilling association). As a result of today's majority opinion, the government may surreptitiously surveil places of worship, protests, gun ranges, abortion or drug-rehabilitation clinics, union meetings, marital counseling or AA sessions, and celebrations of cultural heritage or LGBTQ+ pride, among numerous other types of sensitive places or gatherings—with no judicial oversight or accountability. Without warrants, the government is free to surveil anyone exercising their First Amendment (or other) rights at the government's whim—using a technology that can identify each individual retrospectively, without any suspicion of criminal activity—and those surveilled will be none the wiser. All of that offends the Supreme Court's instruction that Fourth

Amendment review must be particularly rigorous when First Amendment protections are at risk. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978).

* * *

For the first time since the ratification of the Fourth Amendment, the government is permitted to retroactively surveil American citizens anywhere they go—no warrant needed—so long as it keeps its snooping to a few hours or perhaps a few days. New technologies that collect ever-more-intimate data are becoming integral to daily life in ways we could not have imagined even a short time ago. This fact of modern life—that we cannot know what developments, and what risks posed by those developments, lie just around the corner—should counsel courts to exercise humility. The Supreme Court has guided us to safeguard against novel technologies that may enable government infringement on constitutional rights.

That's what we should do. At the end of the day, upholding the precious freedoms guaranteed by our Constitution is our duty. Because the majority decision fails to honor that duty today, I must, with great respect, dissent.