No. 25-112

In the Supreme Court of the United States

OKELLO T. CHATRIE,

Petitioner,

v.

UNITED STATES,

Respondent.

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

BRIEF FOR AMICUS CURIAE GOOGLE LLC IN SUPPORT OF NEITHER PARTY

MITHUN MANSINGHANI
LEHOTSKY KELLER COHN LLP
629 W. Main St.
Oklahoma City, OK 73102

DREW F. WALDBESER
ADELINE K. LAMBERT
LEHOTSKY KELLER COHN LLP
3280 Peachtree Road NE
Atlanta, GA 30305

SCOTT A. KELLER
Counsel of Record
LEHOTSKY KELLER COHN LLP
200 Massachusetts Ave. NW
Suite 700
Washington, DC 20001
(512) 693-8350
scott@lkcfirm.com

Counsel for Amicus Curiae Google LLC

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTEREST OF AMICUS CURIAE[1]

Google LLC is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of products and services, including the Android and Chrome operating systems, as well as Google Search, Maps, Drive, and Gmail.

Central to resolving the question presented is whether Google users have a privacy interest, protected by the Fourth Amendment, in their Google data such as Location History. Google seeks to assist the Court in resolving that issue by explaining the nature and operation of the Location History service, its experience with geofence searches, and how these facts intersect with this Court's precedent.

Google is also dedicated to protecting the privacy of its users' data. While it complies with valid legal process from law enforcement consistent with statutory and constitutional standards, Google vigorously advocates for robust application of the Fourth Amendment to the modern digital context. It thus filed an amicus brief before the district court in this case. Since Google filed that brief, it has moved to quash many geofence warrants. It has also objected to over 3,000 geofence warrants on constitutional grounds.

In December 2023, Google announced that users who chose to turn Location History on would soon

[1] In accordance with Rule 37.6, no counsel for any party has authored this brief in whole or in part, and no person or entity other than Google or its counsel made a monetary contribution to the preparation or submission of this brief.

begin having this data saved on their device. They could view it directly on their mobile devices through the Timeline feature, accessible through Google Maps. As of July 2025, all Location History data that was previously stored on Google's servers was deleted or migrated to on-device storage, and all newly collected Timeline data is stored on-device. Consequently, Google can no longer respond to geofence warrants based on Location History data.[2]

Google takes no position on whether the warrant in this case satisfied the Fourth Amendment, so it files this brief in support of neither party. But Google firmly believes that, based on the private nature of Location History data, law enforcement was required to obtain a warrant to access that data. The fact that Location History was stored securely in the cloud on Google's remote servers—like myriad other highly personal documents and data—does not vitiate the constitutional protections afforded to this sensitive data.

[2] Unless otherwise noted, this brief describes Location History as it functioned at the time the geofence warrant in this case was executed.

INTRODUCTION AND SUMMARY OF ARGUMENT

Individuals' documents and data stored electronically and securely in remote servers are the modern-day "papers[] and effects" protected by the Fourth Amendment. Though kept on servers in "the cloud," these documents are not publicly accessible. They include things like emails, documents, photographs, and search history stored privately by technology companies like Google. They reveal the most intimate details of a person's life. As relevant to this case, they also included Location History data—a personal journal of one's movements—created with that person's consent, controlled by that person, and subject to deletion by that person. These documents are therefore not ordinary business records maintained by a third party that happen to concern an individual; they are the user's *personal* records. Those papers and effects do not lose Fourth Amendment protection merely because they were stored by Google on behalf of the user.

After *Carpenter v. United States*, there can be little question that "individuals have a reasonable expectation of privacy in the whole of their physical movements." 585 U.S. 296, 310 (2018). That holding fully applies to Google's Location History, which was often more precise and more comprehensive than the cell-site location information at issue in *Carpenter*.

When the warrant in this case was executed, Location History was off by default and was only collected if a user chose to enable it. If enabled, Location History essentially functioned as a digital diary of a person's travels. It provided a detailed view

into the person's private life, from the very personal to the mundane, such as every time a user visited his or her home, a hotel, or a place of worship. Users could review that data and delete some, or all, entries if they wished.

"Geofence" searches of Location History data like the one at issue in this case are unlike traditional warrants, which target an identified suspect based on probable cause. Instead, geofence searches operate in reverse, as law enforcement often lacks a suspect when initiating a geofence search. Law enforcement draws a geographic boundary, picks a timeframe, and demands Location History for *every* Google user whose device happened to report and store a location within that area. When Petitioner challenged the geofence warrant in his case, Google filed an amicus brief to ensure that private digital data stored by its users receives the same constitutional protections applied to non-digital papers and effects. The district court agreed that geofence searches require a warrant and cannot be overly broad, becoming the first federal court to hold that a geofence warrant was unconstitutional.

Since then, Google has objected on constitutional grounds to thousands of overbroad geofence warrants across the country. Many of these overbroad warrants swept in hundreds, sometimes even thousands, of innocent people. State and federal courts have repeatedly granted Google's motions to quash these overbroad warrants. Google successfully challenged a warrant that captured Location History for over one thousand people attending funeral services at the

Islamic Center of New Mexico. Google also successfully challenged a warrant that sought all Location History for users across large portions of San Francisco for a cumulative period of two-and-a-half days. No court would authorize a *physical* search of hundreds of people or places, yet geofence warrants sometimes do so by design. These and other experiences confirm the potentially invasive nature of geofence searches and the need for a neutral magistrate to enforce constitutional requirements like particularity.

The third-party doctrine does not create an exception for the constitutional protections afforded to private documents like Location History merely because the documents are stored in the cloud by Google. This Court's third-party cases—*United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979)—held that an individual does not have a reasonable expectation of privacy in a business's records, over which the individual had no control. *Carpenter* likewise characterized those cases as concerning records over which an individual "could 'assert neither ownership nor possession,'" but instead were the "business records of the [third-party]," 585 U.S. at 308 (quoting *Miller*, 425 U.S. at 440)). *Carpenter* nonetheless held that the third-party doctrine did not extend to cell-site location information because of the sensitive nature of that data, *id.* at 309-15. Meanwhile, the dissenters in *Carpenter* argued that the third-party doctrine applied to cell-site location information because cell phone customers "do not create the records; they have

no say in whether or for how long the records are stored; and they cannot require the records to be modified or destroyed." 585 U.S. at 331-32 (Kennedy, J., dissenting). But Location History was entirely different in nature: it was created by Google *users* who, if they chose for Google to record it at all, retained the power to review, edit, and delete it. *Miller* and *Smith* therefore do not apply to Location History.

Documents and data privately housed in the cloud, like the Location History in this case, "are 'such a pervasive and insistent part of daily life' that" they are functionally "indispensable to participation in modern society." *Carpenter*, 585 U.S. at 315 (citation omitted). In the founding era, people stored their constitutionally protected "papers" and "effects" in a desk drawer, a chest, or underneath a mattress. U.S. Const. amend. IV. Now they store them in the cloud. But changes to how people store their papers does not undermine the constitutional protection afforded to those items. Users store these private files on remote servers, behind password-protection, and retain the ability to access, delete, or revise. The fact that they were stored on remote servers rather than the user's specific device should not eliminate Fourth Amendment protections. Emails stored in Gmail are just as private as the letters sent and received by the Framers' generation. Americans do not have to forego technological innovation in order to retain their basic constitutional rights.

To the extent relevant, other sources of law confirm Google users' strong privacy interest in digital data like Location History. Google's Terms of Service

and Privacy Policy promise users that Google will not disclose user data to third parties except in limited circumstances, including in accordance with applicable laws, such as the Fourth Amendment. The Stored Communications Act also reflects Congress's judgment that a warrant is required before internet providers must turn over the "contents" of electronic communications. 18 U.S.C. § 2703(b)(1). Location History qualifies as such content, because it is a journal of a user's movements that the user has asked Google to privately record and store for the user's benefit.

Google takes no position on whether the warrant in this case satisfied the Fourth Amendment. But it urges the Court to hold that Google Location History and other similar digital documents stored remotely deserve the Fourth Amendment's protection. A contrary rule would leave the intimate details of millions of Americans' daily lives—data that will exist in many forms as technology rapidly develops—exposed to warrantless surveillance.

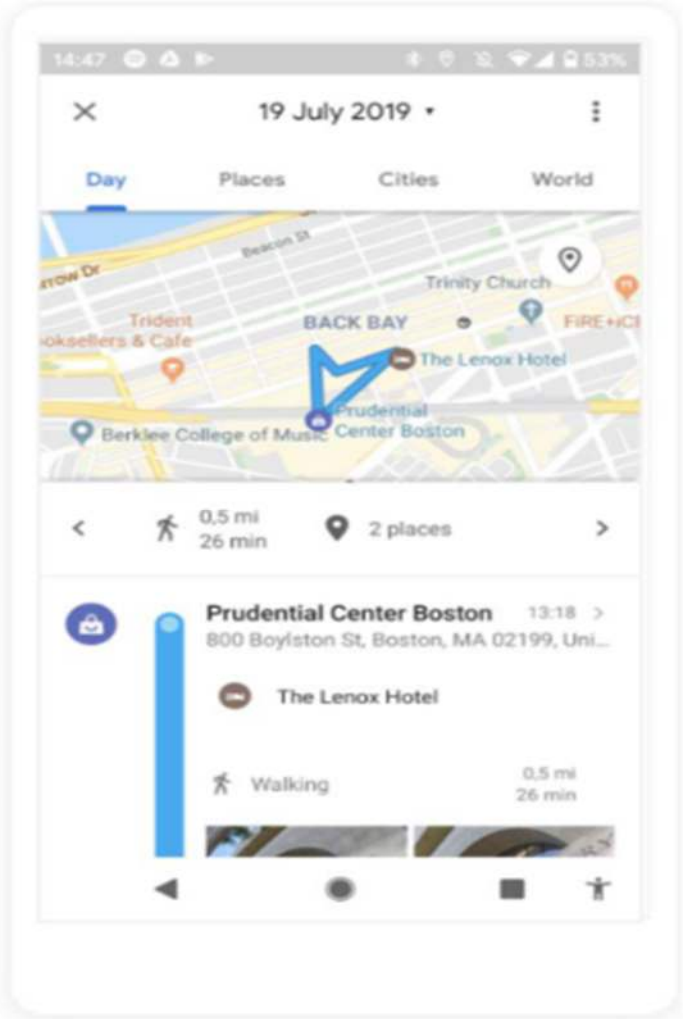
ARGUMENT

I. The Nature of Google Location History and Google's Experience with Geofence Searches.

A. Google enabled users to create and control their Location History data, providing a detailed journal of their location and daily life.

If a user enabled Google's Location History service, their mobile device would automatically upload its physical location to the user's Google account to create an editable chronological record of where their device traveled. Users who chose to store their Location History data in their account could then review that history to remind themselves of a restaurant they ate at two weeks ago, the time they were last at a friend's home, the sites they saw on vacation, or the distance they walked on a particular day.

Location History provided users with a play-by-play virtual journal of their whereabouts over a period of time, which could be displayed on the Google Maps app. This feature provided users with a day-to-day, hour-by-hour, visualization of their movements detailing when, where, and how they traveled with their phones. In essence, the user created a journal. The following screenshot illustrates what a typical entry looked like:


19 July 2019
Day
Places
Cities
World
Trinity Church
BACK BAY
The Lenox Hotel
Prudential Center Boston
0,5 mi
26 min
2 places
Prudential Center Boston
800 Boylston St, Boston, MA 02199, Uni...
The Lenox Hotel
Walking
0,5 mi
26 min

JA.16.

Location History was comprehensive and could be precise. It could estimate a device's location to within "approximately twenty meters or less." JA.45. Location History achieved that accuracy by estimating a device's location not only through nearby cell sites but also through GPS signals and signals from nearby Wi-Fi networks and Bluetooth devices. *Id*. Location History could provide a detailed diary of everywhere a person went: from her house to her gym to her place of worship.

Location History also functioned like a diary in that users decided whether Google recorded and stored Location History or stopped recording altogether. JA.44; JA.95. Google users could review, edit, or delete their Location History information from Google's servers at will, including deleting individual days or all their Location History at once. Users could also instruct Google to automatically delete Location History after a set period of time. JA.46. After the district court's decision in this case, Google announced that, by default, Location History would be auto-deleted after 18 months. *See* Google, *Keeping your private information private* (June 24, 2020), https://perma.cc/8F74-ZMCH.

At the time of the district court's decision in this case, Google stored Location History on its servers. Pet.App.272a. In December 2023, Google announced that users who chose to turn Location History on would soon begin having this data saved on their mobile device, meaning Google would no longer have the ability to access that data. *See* Marlo McGriff,

Updates to Location History and New Controls Coming Soon to Maps, Google: The Keyword (Dec. 12, 2023), https://perma.cc/CW93-X9DN. As of July 2025, all users who chose to record this data migrated to on-device storage, which they can access through the Timeline feature in the Google Maps app. Google now lacks the ability to search for and produce user Location History to law enforcement and Google no longer has the ability to respond to geofence warrants.

B. Google's experience responding to geofence searches from law enforcement shows these searches are invasive and often overbroad.

Given the private nature of Location History, Google has repeatedly advocated for constitutional protections for Location History data. That advocacy has included legal objections to overbroad geofence searches by law enforcement. Google's experience with geofence searches revealed many geofence warrants were extremely overbroad.

1. Unlike traditional warrants, geofence requests are not tied to any particular person, user, or account. They are a type of "reverse warrant": Rather than identifying probable cause to seek data for a particular user, geofence warrants seek data on *every* user who recorded and stored their Location History as placing them within a given location and timeframe precisely *because* law enforcement lacks probable cause that a particular individual committed a crime. Pet.App.53a & n.7 (Wynn, J., concurring). In other words, "the very point of a geofence is to generate leads where none exist." *Id.*

By their nature, geofence searches often run a high risk of sweeping in innocent users—sometimes thousands of them. The searches can vary greatly in the spatial and temporal scope. They might cover two hundred square feet or several square miles; they might span a few minutes or several days. Even a small geographic area for a short period of time can include hundreds or thousands of people, such as geofences covering urban areas during the workday. Law enforcement often defines geofence parameters that cover significantly more ground than the location of the crime being investigated. It is common for a geofence to cover private homes, apartment buildings, government buildings, hotels, places of worship, busy roads, and other locations that law enforcement has not identified particularized probable cause to search.

Google submitted an amicus brief to the district court in this case, explaining the technology and service, and arguing that users have a reasonable expectation of privacy in their Location History data, which deserves constitutional protection. JA.1. Google did not take a position on the constitutionality of this particular geofence warrant, and it filed in support of neither party. Google instead argued that the Fourth Amendment's warrant and particularity requirements apply to geofence searches. *Id.* The district court became the first federal court to hold that a geofence warrant was unconstitutional because it lacked particularized probable cause. Pet.App.265a.

2. After the district court's decision, Google began objecting to overbroad geofence warrants on constitutional grounds. Since 2022, Google has

objected to over 3,000 geofence warrants. When Google still stored Location History on its servers, Google would typically respond to overbroad geofence warrants by sending a letter to law enforcement explaining its constitutional concerns with the warrant and refusing to comply with the warrant as written. For over 2,500 such warrants, law enforcement never responded, essentially withdrawing those warrants. In most of the remaining cases, Google reached an agreement with law enforcement to narrow or withdraw the warrant.

Sometimes, however, law enforcement refused. When law enforcement insisted on an overbroad warrant, Google sought a court order quashing the warrant. Because the warrants are often part of an ongoing criminal investigation, these proceedings are usually sealed. But several subsequently unsealed examples—all of which Google refused to comply with and were then quashed or withdrawn—illustrate how invasive these geofence warrants can be.

In one example, the geofence warrant covered several search areas for a combined 2.5 square miles of San Francisco for a cumulative period of two-and-a-half days. This geofence warrant would have exposed the Location History of *thousands* of users, many of whom "may have been enjoying the privacy of their homes, taking part in protected religious activity in a place of worship, commuting, or engaging in countless other private activities." Order to Partially Seal Records in Sealed Case, Ex. A at 1, *In re Google*, No. 3:25-MJ-70146, ECF 1 (N.D. Cal. Feb. 7, 2025). Google refused to comply with the warrant and moved to

quash it. The government subsequently withdrew the search warrant and Google's motion to quash was denied as moot. *Id.*, Ex. C.

In another case, the warrant sought data from seven search areas spanning 489 acres in Albuquerque, New Mexico. The warrant would have covered over 3,000 users, including over a thousand people attending a funeral service. Google LLC's Mot. to Quash Search Warrant at 1-2, *In re Search of Information Stored at Premises Controlled by Google*, No. 22-mr-1161, ECF 10 (D.N.M. Sept. 7, 2022). After Google filed a motion to quash, law enforcement withdrew the warrant. Order Quashing Search Warrant as Moot, *In re Search of Information*, *supra* ECF 16. Google did not produce any data in response to this warrant.

The following pictures from Google's motion to quash demonstrate how broad the requested searches were:

Google LLC's Mot. to Quash Search Warrant, Ex. C at 1, *In re Search of Information*, *supra*.

Location 1 (above) covered a dense residential neighborhood in Albuquerque, New Mexico. The search area included approximately 170 residential homes and part of a major roadway for one hour in the evening.

Id. at 2.

Location 2 (above) covered another dense residential neighborhood in Albuquerque, and includes over 150 residential homes, 8 apartment complexes, a chapel and cemetery, and a social services organization for one hour.

Id. at 3.

Location 3 (above) covered approximately 200 homes, major roadways, a church, and a community center for one hour.

Id. at 4.

Location 4 (above) significantly overlapped with location 2, but for a different time period, and included over 100 homes and 8 apartment complexes, the same church and cemetery, and multiple roadways.

Id. at 5.

Location 5 (above) covered a three-hour period on a Friday afternoon, during which the funerals took place. In addition to the Islamic Center of New Mexico, the area also included over 50 homes, 30 apartment buildings, a park, major roadways, and a portion of a University of New Mexico parking lot.

Id. at 6.

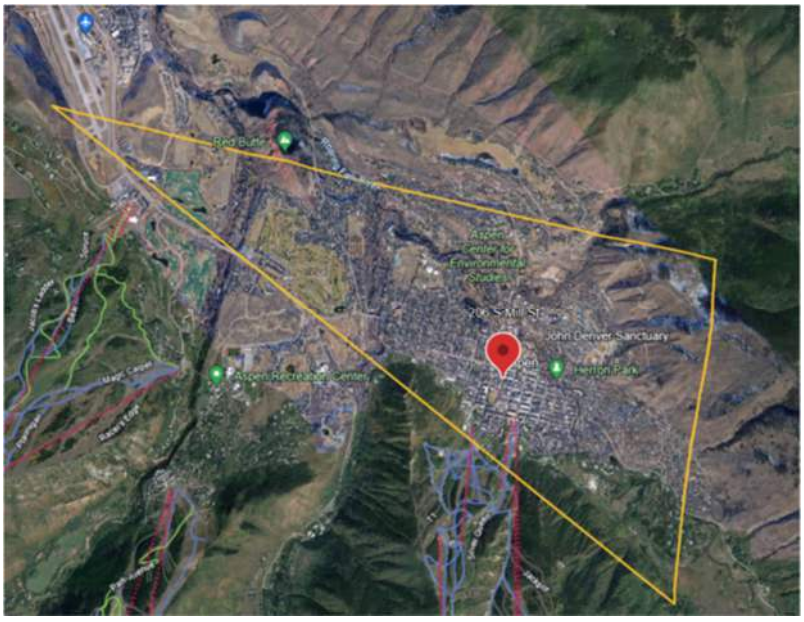
Location 6 (above) covered a dense residential neighborhood with over 100 homes, a church, a ten-story commercial building, and various businesses for one hour.

Id. at 7.

Location 7 (above) significantly overlapped with location 6 and covered one hour later the same evening.

Despite the breadth of these geofences, the primary suspect's device was not even among them, as he had not enabled Location History. Google LLC's Mot. to Quash Search Warrant at 1-2, *In re Search of Information Stored at Premises Controlled by Google*, No. 22-mr-1161, ECF 10 (D.N.M. Sept. 7, 2022).

In another example, Google received a geofence warrant seeking Location History data for 25 square miles over Vail and Aspen, Colorado—sweeping in hundreds of homes, nearly 80 hotels, numerous places of worship, at least two hospitals, and countless other sensitive locations. *See* Google LLC's Mot. to Quash Search Warrant at 2, *In re Matter of Court Order for Production of Records to Google LLC*, No. 2023C30237 (Eagle County, Colo. Oct. 19, 2023). Again, Google refused to comply with the geofence and moved to quash the warrant. The following pictures from Google's motion to quash illustrate the scope of the requested geofence:



Id. at 8.

Location 1 (above) covered nearly all of Aspen, Colorado, including 29 hotels, two ski resorts, the local airport, portions of US Route 82, and the vast majority of homes and businesses in Aspen for three hours in the evening.

Id. at 6.

Location 2 (above) covered nearly 20 square miles over Vail, Colorado. The geofence included nearly every home and business in Vail, Colorado, including 48 hotels, several ski resorts, four churches and two synagogues, and portions of Interstate 70 for two hours in the evening. The court granted Google's motion to quash, and Google did not produce any data in response to this warrant. Order at 1, *In re Matter of Court Order for Production of Records to Google LLC*, No. 2023C30237 (Eagle County, Colo. Dec. 11, 2023).

There are further examples:

- Another geofence warrant requested a search of 330 acres of suburban Wisconsin, encompassing single family homes, major roadways, schools, churches, parks, banks, and restaurants and covering hundreds of users. Google LLC's Memo. In Support of Mot. To Quash, *In re Warrant for Communications/Records Held By: Google LLC*, No.22-GF-13 (Calumet Cty. Circuit Ct., Wis. Nov. 2, 2022). Google refused to comply and moved to quash the warrant. The court granted Google's motion to quash, holding that "[h]ere, as in *Chatrie*, the Geofence authorizes the search of every person in a particular area (including those within a private residence who have a heightened expectation of privacy) and lacks probable cause to search each of these targets." Order Quashing Warrant, No.22-GF-13, at 1, Doc. 35 (Calumet Cty. Circuit Ct., Wis. Nov. 16, 2022).
- Google also received a geofence warrant seeking a search of 84 acres of land in densely populated commercial and residential areas, covering hundreds of users during a busy Memorial Day weekend. Order Quashing Search Warrant at 2, *In the Matter of Court Order for Production of Records to Google LLC*, No. 23-cv-230 (Arapahoe Cty, Colo. Dec. 4, 2023). The court granted Google's motion to

quash the warrant for lack of "probable cause and particularity" because "it will certainly encompass the Location History of many people that are clearly unrelated to criminal activity." *Id.* at 17.

- Google received a geofence warrant asking for a search of 70 acres in a densely populated area over a 24-hour period and covering over 1,500 users. Google again refused to produce the data and moved to quash the warrant. Memo. of Points & Authorities in Support of Google LLC's Ex Parte Petition to Void Search Warrant, *In re Search Warrant to Google LLC*, at 14 (San Joaquin, Cal. Superior Ct. Sept. 12, 2022). The Court voided the search warrant after the government stipulated to withdraw it. Minute Order, *In re Search Warrant to Google LLC*, (San Joaquin, Cal. Superior Ct. Sept. 26, 2022).

These and other examples demonstrate the often intrusive and overly broad nature of geofence searches and other "reverse" warrants—and the need for a particularity requirement so that courts can police them.

II. The Fourth Amendment Protects Google Location History Data.

Google's users have a strong expectation of privacy in their Location History data. Google Location History data was even more comprehensive, precise, and revealing than the cell-site location information this Court held constitutionally protected in *Carpenter*, 585 U.S. at 310-13. Moreover, as Google's motions to quash illustrate, geofence warrants have the potential to ensnare hundreds or thousands of people. *Carpenter*, by contrast, involved a targeted search of the cell site location information for Carpenter only. *See* 585 U.S. at 316 (offering no view on the constitutionality of "tower dumps,"—"a download of information on all the devices that connected to a particular cell site during a particular interval"). Meanwhile, the third-party doctrine from *Smith* and *Miller* is even less applicable to Location History data than it was to the cell-site records in *Carpenter*. The Fourth Amendment therefore requires law enforcement to obtain a warrant based on *particularized* probable cause before the government may obtain a user's Google Location History.

A. Google users have a reasonable expectation of privacy in their Google Location History.

1. *Carpenter* dictates that Google users have a reasonable expectation of privacy in their Location History data. *Carpenter* held that cell-phone users had a reasonable expectation of privacy over cell-site location information, because it provided "an all-encompassing record of the holder's whereabouts,"

allowing the government to peer into a person's "familial, political, professional, religious, and sexual associations." 585 U.S. at 310-11 (quotation omitted). That is doubly true of Google Location History data.

"[I]ndividuals have a reasonable expectation of privacy in the whole of their physical movements." *Carpenter*, 585 U.S. at 310. "[S]ociety'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 for "a very long period." *Id.* at 310 (quoting *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring)). Americans thus enjoy that same degree of privacy against government surveillance even when new technologies "enhance[] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes." *Id.* at 305 (citing *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

"Allowing government access to cell-site records contravenes that expectation." *Id.* at 311. Cell-site location information permitted law enforcement to "track[] nearly exactly the movements of" the user by enabling them to "pinpoint a phone's location within 50 meters." *Id.* at 311, 313. Because individuals "compulsively carry cell phones with them all the time," law enforcement can use cell-site location information to effortlessly "reconstruct a person's movements" as if they had "effectively been tailed every moment of every day for five years." *Id.* at 311-12. Cell-site location information thus provided law enforcement a "detailed log of [the user's] movements,"

and it invaded the user's "reasonable expectation of privacy." *Id.* at 312-13.

That same logic applies to Google Location History. When a user chose to turn on Location History, "Location History data [wa]s . . . more 'detailed' and 'encyclopedic'" than cell-site location information. Pet.App.119a (quoting *Carpenter*, 585 U.S. at 309) (Wynn, J., concurring); *see also United States v. Beverly*, 943 F.3d 225, 230 n.2 (5th Cir. 2019) ("CSLI should not be confused with GPS data, which is far more precise location information derived by triangulation between the phone and various satellites."). Cell-site records narrow location to dozens or hundreds of city blocks. *See Carpenter*, 585 U.S. at 324 (Kennedy, J. dissenting). Google Location History, which relied on GPS and other signals, could pinpoint a device's location within twenty meters. *Supra* p.10; Pet.App.104a (Berner, J., concurring).

In addition, cell-phone service providers collect data only when a cell phone user places or receives a call. Pet.App.208a (Wynn, J., concurring) (explaining if there is "no call," then "no data" is collected with cell-site location information). By contrast, Google Location History recorded the user's location on an ongoing basis, including when the device was not in active use. Pet.App.51a (Diaz, J., concurring); Pet.App.104a (Berner, J., concurring).

Location History was also at least as easy for police to access as cell-site location information. In *Carpenter*, the government needed a suspect's phone number to request that individual's records. *See* 585 U.S. at 301-02. A geofence warrant, however, requires

no suspect at all. "With just the click of a button" and "at practically no expense" to the government, police can rummage through the Location History of hundreds or thousands of users simultaneously. *Id.* at 311. Indeed, the very point of a geofence warrant is to generate leads where none exist—to search first and identify suspects later.

Like cell-site location information, Location History can thus also provide "an all-encompassing record of the [user's] whereabouts," including "his 'familial, political, professional, religious, and sexual associations.'" *Id.* (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). Everywhere a person goes is recorded. Location History thus gives law enforcement a detailed map of a person's life. When the government seizes Location History, it therefore "invade[s the user's] reasonable expectation of privacy in the whole of his physical movements." *Id.* at 313.

2. Google's experience confirms that geofence searches must be subject to the particularity requirement of the Fourth Amendment. As demonstrated above in Part I.B., geofence warrants routinely yield the private data of hundreds or thousands of users. Even worse, they sometimes cover *only* unrelated users—as the perpetrator is not always included in the data set. *See* Google LLC's Mot. to Quash Search Warrant at 1-2, *In re Search of Information Stored at Premises Controlled by Google*, No. 22-mr-1161 (D.N.M. Sept. 7, 2022) (geofence search identified over 3,000 users but suspect was not included in dataset because he had not enabled Location History). If a person happens to be

prosecuted for the crime, those innocent users' data may then be turned over to the accused in discovery, as happened in *Chatrie*. *See* Notice of Satisfaction with Google Response to Subpoena Duces Tecum, *United States v. Chatrie*, No. 3:19-cr-130, ECF 97 (E.D. Va. Mar. 12, 2020).

This Court would almost certainly disapprove of a warrant authorizing *physical* searches of this scope. The government cannot indiscriminately search all persons found in relative proximity to criminal activity. *See Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). Nor can it "search every unit in an apartment building because it has probable cause to believe that some unknown part of the building holds evidence of a crime." Pet.App.123a (Berner, J., concurring). A warrant to search dozens or hundreds of city blocks would not be sufficiently particularized.

This Court therefore should hold that law enforcement must obtain a warrant that complies with the Fourth Amendment's particularity requirement in order to access Location History. A contrary rule would deny individuals core constitutional protections in highly private data.

B. The third-party doctrine does not apply to user data stored by Google, which included Location History.

Carpenter clarifies that citizens have a reasonable expectation of privacy in the type of information contained in Google Location History and similar types of user data. The third-party doctrine from *Smith* and *Miller* should not be extended to Google Location History just because this data (formerly) resided on Google's servers. Such an extension of the third-party doctrine would ignore seismic shifts in how citizens store their "papers and effects." "[I]t would be a grave misjudgment to conflate an individual's limited disclosure to Google with an open invitation to the state." Pet.App.64a-65a (Wynn, J., concurring).

1. The third-party doctrine does not apply to Google Location History under either the *Carpenter* majority or dissenting views. These records are stored in the *user's account* by Google and are created and controlled by the user. This is not a *business's record* created from information disclosed by a customer and generally not subject to the customer's control.

This Court's third-party doctrine cases hold that when individuals share information with a business, the individual has no reasonable expectation of privacy in *that business's* records. *Miller* thus held that a person had no reasonable expectation of privacy in financial information conveyed to banks, because "the documents subpoenaed" were "the business

records of the banks." 425 U.S. at 440-41. The information was "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," so the individual had no "legitimate expectation of privacy concerning the information kept in bank records." *Id.* at 442. When a depositor hands cash to a bank teller, the bank creates its own ledger entries. Those records belong only to the bank—the depositor cannot prevent their creation, modify them, or delete them. The bank's copies of checks were not "private papers" or "confidential communications but negotiable instruments to be used in commercial transactions." *Id.* at 440, 442 Similarly, in *Smith*, telephone numbers dialed by an individual were recorded by the phone company to ensure accurate bills, so the individual had no reasonable expectation of privacy in those business records. 442 U.S. at 734-44.

Carpenter confirmed that the third-party doctrine is limited to records created and controlled by the businesses.[3] The *Carpenter* majority described *Miller* as rejecting a Fourth Amendment challenge because the defendant "could 'assert neither ownership nor possession' of the documents; they were 'business records of the banks.'" 585 U.S. at 308 (quoting *Miller*, 425 U.S. at 440)). The dissenters disagreed that *Carpenter* had a reasonable expectation of privacy in

[3] *Carpenter* ultimately held that even some records controlled by a business, like cell-site location information, deserve Fourth Amendment protection because they are a qualitatively different category of record that present fundamentally different private concerns. 585 U.S. at 313.

that case, yet they nevertheless agreed that *Miller* and *Smith* stand for the proposition that "individuals lack any protected Fourth Amendment interests in records that are *possessed, owned, and controlled* only by a third party." 585 U.S. at 327 (Kennedy, J., dissenting) (emphasis added). The *Carpenter* dissenters thus would have found customers "have no reasonable expectation" of privacy in cell-site location information because they "do not own, possess, control, or use the records." *Id.* at 322. Nothing "provide[d] customers any practical control over the records" and "[c]ustomers do not create the records; they have no say in whether or for how long the records are stored; and they cannot require the records to be modified or destroyed." *Id.* at 331-32. A separate dissenting opinion likewise reasoned that "the Government did not search Carpenter's property" because "[h]e did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them." *Id.* at 342 (Thomas, J., dissenting); *see id.* at 405.

None of this is true of Google Location History, so it falls outside the third-party doctrine under both the *Carpenter* majority and dissenting views. As already explained, Google's *users* decided whether to create Location History. *Supra* p.10. They could control it, view it, download it, delete individual days or the entire dataset, and pause or revoke collection at any time. *Supra* p.10. The third-party doctrine simply does not apply when the user retains substantial dominion over data entrusted to a custodian for safekeeping. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (rejecting the third-party doctrine where a

provider stored emails and explaining that "the best analogy" was to "'cases in which a third party carries, transports, or stores property for another'" (quoting Bellia & Freiwald, *Fourth Amendment Protection For Stored E–Mail*, 2008 U. Chi. Legal F. 121, 165 (2008))). This is thus an even easier case than *Carpenter*, since cell-site location information was far more like the business records at issue in *Miller* and *Smith*.

2. The third-party doctrine also does not apply to Google Location History because, just like cell phone usage in *Carpenter*, cloud storage of personal information on third-party servers is an indispensable part of modern life and can provide intimate insight into a person's private actions.

Google stored information for users on remote servers, but that "does not mean that the Fourth Amendment falls out of the picture entirely." *Riley v. California*, 573 U.S. 373, 392 (2014). The mere fact that cell-site "records are generated for commercial purposes," for example, did "not negate Carpenter's anticipation of privacy." *Carpenter*, 585 U.S. at 311. Rather, cell phones and the services they provide are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." 585 U.S. at 315 (quoting *Riley*, 573 U.S. at 385). Unlike "the limited types of personal information addressed in *Smith* and *Miller*"—bank records and phone numbers dialed—"the exhaustive chronicle of location information casually collected by wireless carriers" was different in kind. *Id.* at 314. It "is an entirely different species" of business record—something that implicates basic Fourth Amendment

concerns about arbitrary government power "much more directly than corporate tax or payroll ledgers." *Id.* at 318.

This same logic applies to Google Location History. Digital services like those offered by Google are used by virtually every American. *See Riley*, 573 U.S. at 385. A person cannot opt out of all these services—email, cloud storage, search engines—and still participate in modern life to the same degree. This online information is also "deeply revealing," given its huge "depth, breadth, and comprehensive reach." *Carpenter*, 585 U.S. at 320.

The *Carpenter* dissenters acknowledged the third-party doctrine "may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party." 585 U.S. at 332 (Kennedy, J., dissenting) (citation omitted). Personal documents and data stored securely by digital service providers are the modern-day equivalent of "papers" or "effects" protected by the Fourth Amendment. U.S. Const. amend. IV. This Court has already recognized that digital files are protected by the Fourth Amendment if they are stored on a cell phone. *Riley*, 573 U.S. at 386. And it further recognized that a search of a cell phone could "extend well beyond papers and effects" in the physical world because the cell phone can access user "data stored on remote servers rather than on the device itself." *Riley*, 573 U.S. at 397-98. As a result, the Fourth Amendment should protect "files stored in the cloud" even if law enforcement seizes a phone, because a search of the

cloud "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." *Id.* It would make little sense for files stored on a cell phone (as is now the case with Timeline data) to be protected, but *the same files* stored in the cloud to be treated differently.

Individuals do not lose a reasonable expectation of privacy in letters simply because they are held by a mail carrier. *Ex parte Jackson*, 96 U.S. 727, 733 (1878). By the same token, *digital* letters (emails) do not lose their constitutional protections simply because they are held by an email provider or transmitted by an internet service provider. *Warshak*, 631 F.3d at 274. Meanwhile, Location History is the modern-day equivalent of a travel journal, and it should be treated the same. The fact that people now store their "papers" and "effects" on remote servers does not make them less worthy of constitutional protection. These are user-specific private records, inaccessible to the public, protected with passwords, that are created and controlled by the user.

A contrary ruling would severely erode the Fourth Amendment in the digital age given the vast "quantities of personal information" preserved by using these personal services. *Riley,* 573 U.S. at 386. If Location History loses Fourth Amendment protection simply because a user consents to their information residing on a third party's servers, the same logic would strip constitutional protection from emails stored in Gmail, documents, photographs, and ledgers in Google Drive, Google search histories, and text message backups. In all these contexts, users

create data and entrust it to a technology company for safe and private storage.

Disclosing such information to the government would also chill core First Amendment activities. Digital journals and search queries reflect a user's most private thoughts and practices. Emails, Google Drive documents, search histories, and, of course, Location History could reveal a user's associations and group memberships. The government could use this information to target searches based on Google users' speech contained in their stored documents, emails, and search histories. Clear guidance from this Court will thus vindicate not only Fourth Amendment principles, but additional constitutional freedoms.

III. Other sources of law reinforce that users have a reasonable expectation of privacy in Google Location History.

The contracts and statutes applicable to Google Location History corroborate user's constitutionally protected expectation of privacy in their Google data. Google's Terms of Service and the Stored Communications Act confirm that law enforcement needs a valid warrant to obtain Location History.

A. Google's Terms of Service and Privacy Policy protect user privacy, including from unlawful government intrusion.

As a threshold matter, Google's Terms of Service and Privacy Policy—contracts between two private parties—should not control the constitutional questions in this case. But some courts in related contexts have wrongly held that Terms of Service impact whether an individual has a reasonable expectation of privacy. This Court should clarify that private contracts do not alter a user's constitutional rights.

Private "[a]greements cannot create Fourth Amendment rights. Nor can they take them away." Orin S. Kerr, *Terms of Service and Fourth Amendment Rights*, 172 U. Pa. L. Rev. 287, 308-13, 328 (2024). Private contracts over shared spaces "concern risk allocation between private parties," and they have little to do with Fourth Amendment rights. *Byrd v. United States*, 584 U.S. 395, 408 (2018). A hotel guest that permits housekeeping to enter his room does not thereby consent to a police search. *See Stoner v. California*, 376 U.S. 483, 489 (1964). Nor does a tenant that allows a landlord to monitor the property for waste consent to a landlord-led search by law enforcement. *Chapman v. United States*, 365 U.S. 610, 617 (1961).

Despite that precedent, some courts have suggested that Terms of Service are a "rights contract: by agreeing to use the service, they reason, you agree to whatever narrowing or elimination of rights that the contract implies." Kerr, *supra*, at 289 (describing

this line of cases). For instance, *Commonwealth v. Dunkins* held that a student abandoned his Fourth Amendment rights in data stored on the college Wi-Fi network because he agreed to Terms of Service allowing the college to disclose the records to law enforcement. 669 Pa. 456, 469 (2021). *United States v. Adkinson* similarly held that a defendant had no privacy interest in his cell site location information because he "agreed to T-Mobile's policy that T-Mobile could disclose information when reasonably necessary." 916 F.3d 605, 610 (7th Cir. 2019). *State v. Pauli* found a user had no reasonable expectation of privacy in files stored on DropBox because "the terms of service prohibited illegal activity, permitted the provider to review user activity and content, and permitted the provider to report violations of their terms and other law to third parties." No. A19-1886, 2020 WL 7019328, at *3 (Minn. Ct. App. Nov. 30, 2020).

Those cases ignore this Court's precedents about private contracts and Fourth Amendment rights. Worse, the rule adopted by these cases would nullify Fourth Amendment protections for most internet-related activity. Terms of Service are "a pervasive and insistent part of daily life." *Riley*, 573 U.S. at 385. Americans routinely agree to Terms of Service on every online service they use. These private contracts outline the service's expectations for users and users' expectations for the service. People may agree to grant providers access to their communications or data for a limited, clearly defined set of purposes, such as abuse detection, fraud prevention, internal diagnostics, or

enforcement of community guidelines. But an agreement to grant a provider access is not an invitation to the government to comb through a person's inbox.

Given their ubiquity, the "American populace" may have a "certain level of comfort . . . 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." Pet. App. 233a (Wynn, J., dissenting). An online provider's right to access or use subscriber information under its Terms of Service "does not diminish the reasonableness of [the user's] trust in the privacy of his" data. *Warshak*, 631 F.3d at 287. That is doubly true because Terms of Service vary service to service and can change frequently. A person's Fourth Amendment privacy rights should not depend on a patchwork of contractual rights that shift depending on which online services he uses.

Even if Google's Terms of Service were relevant to the constitutional analysis, they confirm that Google users have a reasonable expectation of privacy in their data. Google's Privacy Policy specifically says that Google will not share users' personal information except in specific circumstances, like complying with lawful and enforceable warrants. JA.69-70. A privacy policy that accurately informs a user about legal obligations related to disclosures cannot constitute a user's consent to a lower level of protection than what the Constitution requires. Indeed, the Terms of Service expressly confirm that "[t]he Fourth

Amendment to the US Constitution and the Electronic Communications Privacy Act (ECPA) restrict the government's ability to force a provider to disclose user information." Google, *Privacy and Terms*, https://perma.cc/W5LX-EEV8 (last accessed Feb. 27, 2026). Google will not disclose "the content" of user data without a search warrant. *Id.* Google takes that commitment seriously, as its challenges to overbroad geofence warrants confirm.

In short, Google makes express commitments to protect user data from unlawful government access, including access in contravention of the Fourth Amendment. This Court has never used such a contract as a basis to deny a person Fourth Amendment protections under the third-party doctrine, and it should not do so here. Such a ruling would ignore the actual language of Google's Terms of Service, contravene users' clear expectations of privacy, and unnecessarily diminish constitutional rights.

B. The Stored Communications Act reflects Congress's judgment that law enforcement must obtain a warrant to search Google Location History.

The Stored Communications Act ("SCA") allows law-enforcement to compel service providers such as Google to disclose data relating to a user's stored electronic communications. *See* 18 U.S.C. § 2703. But the government must obtain a warrant supported by probable cause before it can require a provider to disclose the "contents" of "electronic communications." *Id.* § 2703(b)(1); *see* H.R. Rep. No. 114-528, at 9 (2016) (explaining that Department of Justice has, since 2013, followed judicial precedent requiring a warrant to access the contents of all electronic communications, despite exceptions to that requirement in the text of the SCA). "[E]lectronic communication[s]" include any "transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part" by "an [electronic] system." 18 U.S.C. § 2510(12). The "contents" of such a communication includes "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

Location History easily qualifies as the "contents" of "electronic communications." 18 U.S.C. § 2703(b)(1). Location History recorded where Google's users traveled and when. When Google stored Location History on its servers, that data was "transfer[ed]" to Google. 18 U.S.C. § 2510(12). And the "substance, purport, [and] meaning" of the stored information is the digital journal that the service provided. When a

user opted in to Location History, she intentionally communicated to Google her location information so that Google could store it for her.

To be sure, some courts have described cell-site location information as "non-content information." *United States v. Graham*, 824 F.3d 421, 425 (4th Cir. 2016). But Location History is different. It is not metadata produced as an ancillary byproduct of another electronic communication. A user's individual Location History instead "comprises" the "communication's substance" because it is a digital diary of locations that users ask Google to record and store. *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 136 (3d Cir. 2015). Location History therefore qualifies as the "contents" of "electronic communication." 18 U.S.C. § 2703(b)(1); *id.* § 2510(8). Under the SCA, law enforcement can obtain it only with a particularized warrant—just as it would need a warrant to compel Google to produce the contents of a user's written journals stored on Google Drive.

Congress's decision to protect electronic information like Location History in the SCA confirms that Google's users have a reasonable expectation of privacy in that data. It constitutes a legislative judgment that, in order to obtain this information, law enforcement must do what they would with searches for any other private papers or effects: get a warrant.

CONCLUSION

This Court should hold that users have a reasonable expectation of privacy in their Google Location History and that law enforcement must comply with the Fourth Amendment's warrant and particularity requirements to obtain this data.

Respectfully submitted,

MITHUN MANSINGHANI
LEHOTSKY KELLER COHN LLP
629 W. Main St.
Oklahoma City, OK 73102

DREW F. WALDBESER
ADELINE K. LAMBERT
LEHOTSKY KELLER COHN LLP
3280 Peachtree Road NE
Atlanta, GA 30305

SCOTT A. KELLER
Counsel of Record
LEHOTSKY KELLER COHN LLP
200 Massachusetts Ave. NW
Suite 700
Washington, DC 20001
(512) 693-8350
scott@lkcfirm.com

Counsel for Amicus Curiae Google LLC

MARCH 2026