UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA v. OKELLO T. CHATRIE, *Defendant*.	Case No. 3:19-cr-00130-MHL

BRIEF OF AMICUS CURIAE GOOGLE LLC IN SUPPORT OF NEITHER PARTY CONCERNING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE FROM A "GEOFENCE" GENERAL WARRANT (ECF NO. 29)

DISCLOSURE STATEMENT

Pursuant to Local Criminal Rule 12.4, Google hereby discloses that it is an indirect subsidiary of Alphabet Inc., a publicly traded company. No publicly traded company holds more than 10% of Alphabet Inc.'s stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES AND RULES

OTHER AUTHORITIES

INTEREST OF AMICUS CURIAE[1]

Google LLC ("Google") 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. Among those products and services is Google Location History ("LH"), which allows individual users who have chosen to use the LH service to create, edit, and save records of their whereabouts over time—akin to journal entries of journeys taken and places visited. The warrant at issue in this motion compelled Google to produce data associated with Chatrie and other Google users—specifically, data from Google's LH service.

When using LH and other services, Google users routinely entrust private, personal data, including location-related information, to Google for processing and storage. Google recognizes and respects the privacy of this information and is transparent with users about when and how their information is stored. For example, Google's Privacy Policy informs users about their data, how to keep it safe, and how to take control. And Google regularly publishes transparency reports that reflect the volume of requests for disclosure of user data that Google receives from government entities.

Google respectfully submits this amicus brief in support of neither party to provide contextual information to the Court about the data at issue in Defendant Chatrie's motion to suppress evidence obtained from a so-called "geofence" warrant. *See* Mot. to Suppress Evidence

[1] The undersigned certifies that no party or party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was used to fund the preparation or submission of this brief; and no persons other than amicus curiae or its counsel contributed money that was intended to fund the preparation or submission of this brief.

Obtained From a "Geofence" General Warrant (ECF No. 29) ("Mot."); Govt. Response in Opp. to Def.'s Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (ECF No. 41) ("Opp."). That warrant compelled Google to produce users' LH information, so an understanding of that information—including what it is, how users can create and save it, and what Google must do to comply with a warrant to produce it—is needed to resolve the parties' legal arguments on the motion to suppress. While the parties' briefs reveal some uncertainty about certain aspects of LH that are relevant to the questions presented by the motion, Google is well situated to explain the nature of the data and the steps Google takes in response to geofence warrants like the one at issue here. Moreover, because law-enforcement requests for this type of data have become increasingly common in recent years, Google also has a significant interest in the constitutional and statutory requirements and limitations that govern law enforcement efforts to obtain LH information. While Google takes no position on the validity of the warrant at issue in this case or whether the evidence it yielded should be suppressed, it respectfully urges the Court to take into account the full factual context surrounding the warrant and hold that both the Stored Communications Act, 18 U.S.C. § 2703, and the Fourth Amendment require the government to obtain a warrant supported by probable cause to obtain LH information stored by Google users.[2]

INTRODUCTION AND SUMMARY OF ARGUMENT

Pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, law enforcement can and frequently does obtain legal process compelling Google to disclose the contents or

[2] By submitting this brief as amicus curiae, Google does not become a party to the case and does not waive any objections it might have to any efforts by the parties to obtain discovery or testimony from Google. *See, e.g.*, Fed. R. Crim. P. 17(c)(2); *In re Grand Jury, John Doe No. G.J.2005-2*, 478 F.3d 581, 585 (4th Cir. 2007) ("Courts have recognized various ways in which a subpoena may be unreasonable or oppressive under Rule 17(c).").

records of particular users' stored electronic communications, including data that reveals those persons' locations and movements at particular times of interest. Such requests typically seek to compel disclosure of information pertaining to specifically identified persons of interest in a criminal investigation.

This case, in contrast, concerns a novel but rapidly growing technique in which law enforcement seeks to require to search across LH data, using legal requests sometimes called "geofence" requests. Rather than seeking information relating to a known suspect or person of interest, these requests broadly seek to identify all Google LH users whose LH data suggests that they were in a given area in a given timeframe—even though law enforcement has no particularized basis to suspect that all of those users played a role in, or possess any information relevant to, the crime being investigated. State and federal law-enforcement authorities have made increasing use of this technique in recent months and years. Year over year, Google has observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and to date, the rate has increased over 500% from 2018 to 2019.

As set forth below, the LH information at issue in geofence requests such as the one in this case differs in significant respects from the cell site location information ("CSLI") at issue in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and other types of data that courts have considered in Fourth Amendment cases. For example, rather than a record created and stored by Google as an automatic result of using a Google service, Google LH information is created, edited, and stored by and for the benefit of Google users who opt into the service and choose to communicate their location information to Google for storage and processing. Moreover, LH information can often reveal a user's location and movements with a much higher degree of precision than CSLI and other types of data. And rather than targeting the electronic

communications of only a specific user or users of interest, the steps Google must take to respond to a geofence request entail the government's broad and intrusive search across Google users' LH information to determine which users' devices may have been present in the area of interest within the requested timeframe.

Given the characteristics of geofence requests, the law requires the government to obtain a warrant to require Google to search LH information. First, although the parties have not addressed the statutory context, the Stored Communications Act ("SCA")—quite apart from the Constitution—requires the government to obtain a search warrant because a geofence request seeks the "contents" of Google users' electronic communications within the meaning of the SCA. *See* 18 U.S.C. § 2703(a), (b). Therefore, regardless of whether a geofence request amounts to a "search" for Fourth Amendment purposes, the government must obtain a warrant from a neutral magistrate that satisfies the requirements of probable cause and particularity. *See id.* (incorporating requirements of Fed. R. Crim. P. 41).

In any event, it is also clear that a geofence request constitutes a "search" within the meaning of the Fourth Amendment and that, absent an applicable exception, the Constitution independently requires the government to obtain a warrant to obtain LH information. Users have a reasonable expectation of privacy in their LH information, which the government can use to retrospectively reconstruct a person's movements in granular detail. Under *Carpenter*, the "third-party doctrine" does not defeat that reasonable expectation of privacy merely because users choose to store and process the information on Google' servers.

Whether under the SCA or under the Fourth Amendment—and absent an applicable exception—the government is therefore obligated to obtain a warrant to search LH information. That requirement is entirely appropriate in light of the sensitivity of LH information, the intimate

details it can reveal about a user's life, and the breadth of the government's intrusion on users' private LH information that occurs whenever a geofence search is executed. Google's users expect their LH information to be kept private, and the Court should ensure that it receives the greatest available protection. Google takes no position on Defendant Chatrie's arguments that the warrant at issue here failed to satisfy the requirements of probable cause and particularity or, if so, whether suppression is the appropriate remedy. But the Court should hold—taking account of the full factual context—that a warrant is indeed required.

ARGUMENT

I. GOOGLE "LOCATION HISTORY" INFORMATION DIFFERS SIGNIFICANTLY FROM CELL SITE LOCATION INFORMATION AND OTHER TYPES OF LOCATION DATA COURTS HAVE CONSIDERED IN OTHER FOURTH AMENDMENT CASES

While many of Google's products and services can be used without a Google account, millions of people choose to create Google accounts and log into them from their mobile devices or while using Google applications to take full advantage of account-specific products such as Gmail and to obtain a more personalized experience on applications such as Maps and Search. Holders of Google accounts can control various account-level and service-level settings and preferences. "Location History" (or "LH") is an optional account-level Google service. It does not function automatically for Google users. But when users opt into LH on their Google accounts, it allows those users to keep track of locations they have visited while in possession of their mobile devices.

In the briefing, the parties analogize the LH information at issue in this case to CSLI, "tower dumps," GPS data, and other types of location information that courts have considered in other cases. Mot. 2, 14; Opp. 7-8, 11-12, 18. In fact, while Google LH information bears some similarities to those types of data in some respects, it differs in important ways that are highly

relevant to the question whether a warrant is required. In determining the legal framework governing law enforcement requests for Google LH information, the court should therefore proceed with an understanding of the nature and precision of that information, how it is recorded and stored, how users control it, and how it is collected in response to legal process.

A. Google "Location History" Is Not A Business Record, But A Journal Of A User's Location And Travels That Is Created, Edited, And Stored By And For The Benefit Of Google Users Who Have Opted Into The Service

Google "Location History" information is essentially a history or journal that Google users can choose to create, edit, and store to record their movements and travels. Google's users activate and use LH for many reasons. By enabling and using LH, a Google user can keep a virtual journal of her whereabouts over a period of time. For most Google users, this journal is captured in the "Timeline" feature of the Google Maps app. *See* Fig. 1. The Timeline feature allows the user to visualize where she has traveled with her phone and when over a given period—in essence, a journal. The Timeline might reflect, for instance, that the user left her home on Elm Street in the morning and walked to the bus stop, took the bus to her office on Main Street, walked to a nearby coffee shop and back to the office in the afternoon, and then went to a nearby restaurant in the evening before returning home by car.

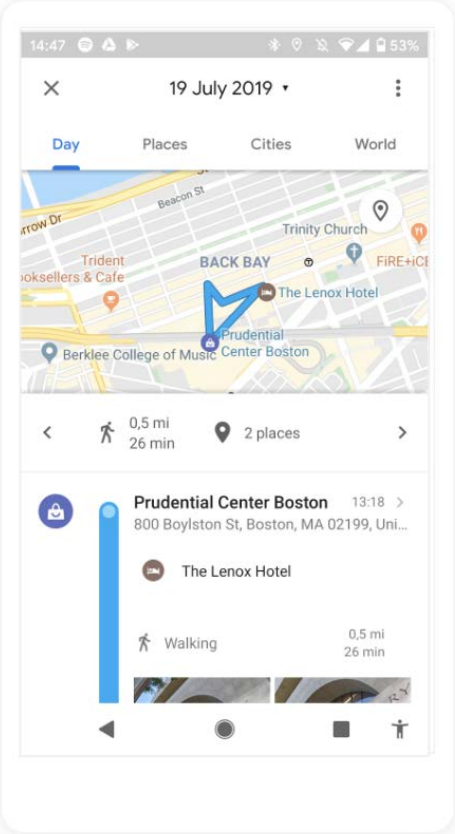

Figure 1. Sample Google Timeline.

By using Google LH, the user can access other benefits on her Google device or applications as well. For example, she can obtain personalized maps or recommendations based

on places she has visited, get help finding her phone, and receive real-time traffic updates about her commute.[3]

For Google LH to function and save information about a user's location, the user must take several steps—some tied to her mobile device, some tied to her Google account. First, the user must ensure that the device-location setting on her mobile device is turned on. When the device-location setting is activated, the mobile device automatically detects its own location, which the device ascertains based on GPS and Bluetooth signals, Wi-Fi connections, and cellular networks.[4] Second, the user must configure her mobile device to share location information with applications capable of using that information. Not all mobile applications can use location information, and those that can, such as Google Maps, will do so only if the user configures her device to allow the app to use the mobile device's location information.

Critically, merely taking the steps described above that are tied to the mobile device does not on its own generate a saved LH record of a Google user's locations. Google does not save information about where a particular mobile device has been to a user's account—even when the device-location feature is turned on and applications on the device are using location data—unless the user has also taken additional specific steps tied to her Google account. Specifically, the user must opt into LH in her account settings and enable "Location Reporting"—a subsetting

[3] *See* Google, *Manage Your Location History*, https://support.google.com/accounts/answer/3118687 (visited Dec. 20, 2019).

[4] Android users can tailor their devices' location-reporting settings, controlling which sources of information (*e.g.*, GPS, cellular, or Wi-Fi) are detectable from the device, and which applications can access location data. *See, e.g.*, Google, *Manage Your Android Device's Location Settings*, https://support.google.com/accounts/answer/3467281 (visited Dec. 20, 2019); Google, *Choose Which Apps Use Your Android Phone's Location*, https://support.google.com/android/answer/6179507 (visited Dec. 20, 2019).

within LH—for the particular device.[5] And to actually record and save LH data, the user must then sign into her Google account on her device and travel with that device. In sum, LH functions and saves a record of the user's travels only when the user opts into LH as a setting on her Google account, enables the "Location Reporting" feature for at least one mobile device, enables the device-location setting on that mobile device, permits that device to share location data with Google, powers on and signs into her Google account on that device, and then travels with it.

When a user takes those steps, the resulting data is communicated to Google for processing and storage on Google's cloud-based servers, and to enable Google to make it available to the user in various ways. But it is the user who controls the LH information. The user can review, edit, or delete her Timeline and LH information from Google's servers at will. For example, the user could decide to keep LH information only for dates when she was traveling abroad and manually delete the rest; she could delete all Timeline entries except those associated with visits to memorable restaurants; she could instruct Google to automatically delete all LH information after a set period (say, every three months); or she could keep all LH information for future reference.

The user thus controls her Google LH data—unlike, for instance, the CSLI at issue in *Carpenter* or cellular data obtained via a "tower dump." As the Supreme Court explained in *Carpenter*, CSLI consists of time-stamped records that are automatically generated by and for the wireless carrier whenever a mobile device connects to a cell site (*i.e.*, the physical radio

[5] A Google account may be associated with multiple devices. The "Location Reporting" feature within LH allows users to select specific devices on which to enable LH. *See* Google, *Manage Your Location History*, https://support.google.com/accounts/answer/3118687 (visited Dec. 20, 2019).

antennas that make up the cellular network). 138 S. Ct. at 2211-2212. Wireless carriers collect and maintain CSLI records "for their own business purposes," such as identifying weak spots in the network or determining when to apply roaming charges. *Id.* at 2212. When law enforcement seeks access to CSLI, it is thus asking the wireless carrier to produce its own business records showing when a particular device connected to a cell site within a particular period of time. A request for a "tower dump" likewise seeks the wireless carrier's own business records—in that case, identifying every phone that connected to a particular cell site (or "tower") in a particular period.

Mobile device users cannot opt out of the collection of CSLI or similar records, nor can they retrieve, edit, or delete CSLI data. Google LH information, by contrast, is stored with Google primarily for the user's own use and benefit—just as a user may choose to store her emails on Google's Gmail service and her documents on Google Drive. Google LH information is controlled by the user, and Google stores that information in accordance with the user's decisions (*e.g.*, to opt in or out, or to save, edit, or delete the information), including to enhance the user's experience when using other Google products and services. *Supra* pp. 6-8.

Defendant thus errs in asserting that "[i]ndividuals do not voluntarily share their location information with Google," Mot. 10, and that the acquisition of user location records by Google is "automatic and inescapable," Reply 6. As discussed, Google does not save LH information unless the user opts into the LH service in her account settings (and logs into her Google account while using a properly configured mobile device), and the user can choose at any time to delete some or all of her saved LH information or to disable the LH service completely. And LH information was the only location information produced to the government in response to this geofence warrant.

B. Google LH Can Reflect A User's Location and Movements More Precisely Than CSLI And Other Types Of Data

Google LH information can be considerably more precise than other kinds of location data, including the CSLI considered in *Carpenter*. That is because, as a technological matter, a mobile device's location-reporting feature can use multiple inputs in estimating the device's location. Those inputs include not only information related to the locations of nearby cell sites, but also GPS signals (*i.e.*, radio waves detected by a receiver in the mobile device from orbiting geolocation satellites) or signals from nearby Wi-Fi networks or Bluetooth devices. Combined, these inputs (when the user enables them) can be capable of estimating a device's location to a high degree of precision. For example, when a strong GPS signal is available, a device's location can be estimated within approximately twenty meters.[6]

CSLI, by contrast, shows a less-detailed picture of a mobile device's movements. Although its precision has increased as wireless carriers have introduced more and more cell towers that cover smaller and smaller areas, it typically reflects location on the order of dozens to hundreds of city blocks in urban areas rather than a matter of meters, and up to forty times more imprecise in rural areas. *See Carpenter*, 138 S. Ct. at 2225 (Kennedy, J. dissenting); *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.").[7]

---

[6] *See* Google, *Find And Improve Your Location's Accuracy*, https://support.google.com/maps/answer/2839911 (visited Dec. 20, 2019).

[7] No estimate is perfect, and the estimated locations reflected in Google LH are no exception. Like any probabilistic estimate based on multiple inputs, the estimated locations reflected in Google LH have a margin of error, so a user's actual location will not always align with any one estimated location data point in LH. In that respect, LH differs from CSLI, which is not an estimate at all, but simply a historical fact: that a device connected to a given cell tower

C. Collecting And Producing Google LH Information To Law Enforcement In Response To A Geofence Request Requires A Uniquely Broad Search Of All Google Users' Timelines

The Stored Communications Act ("SCA") governs how service providers such as Google handle the contents and records of their users' stored electronic communications, including Google LH. In general, the SCA prohibits unauthorized access to those stored communications, restricts the service provider's ability to disclose them to the government, and delineates the procedures law enforcement must follow—and the substantive standards it must meet—to compel a service provider to produce them. *See* 18 U.S.C. §§ 2701 *et seq.*

Typically, U.S. law-enforcement authorities use legal process (whether in the form of a search warrant, court order, or subpoena) to compel Google to disclose content or records of electronic communications associated with specifically identified Google users or accounts. For example, the government might obtain a warrant for the contents of emails associated with a particular Gmail account. Google often receives warrants for LH information that take the same form—*i.e.*, demands for a specifically identified Google user's LH information from a specifically identified time range. When producing data in response to such a demand, Google must search for and retrieve only the responsive data that is associated with the particular users or accounts identified in the warrant.

So-called "geofence" requests operate quite differently. Geofence requests represent a new and increasingly common form of legal process that is not tied to any known person, user, or account. Instead, law enforcement uses geofence requests in an attempt to identify all Google users who might have stored LH data in their accounts suggesting that they were near a given

---

during a given time period. An LH user's Timeline, however, combines and contextualizes numerous individual location data points, so that the resulting picture of the user's location and movements is sufficiently precise and reliable for the purposes for which it was designed.

area in a given timeframe—and to do so at a level of precision not available through CSLI or similar data.

Such requests typically identify a geographic area surrounding a point of interest. That point of interest is typically a suspected crime scene. As Defendant observes (at Mot. 12-13), however, the geographic area can also include private homes, government buildings, places of worship, and other sensitive locations. A geofence request seeks to compel Google to produce LH information for all Google users whose LH records indicate that they may have been present in the defined area within a certain window of time, which might span a few minutes or a few hours. (In practice, although the legal requests do not necessarily reflect this limitation, such requests can cover only Google users who had LH enabled and were using it at the time in question.)

Many of the earliest "geofence" legal requests attempted to mimic "tower dump" requests, seeking LH data that would identify all Google users who were in a geographical area in a given time frame. In light of the significant differences between CSLI and Google LH data described above, however, Google developed a multi-step anonymization and narrowing protocol to ensure privacy protections for its users. That protocol typically entails a three-step process:

First, law enforcement obtains legal process compelling Google to disclose an anonymized list of all Google user accounts for which there is saved LH information indicating that their mobile devices were present in a defined geographic area during a defined timeframe. Google, however, has no way to know ex ante which users may have LH data indicating their potential presence in particular areas at particular times. In order to comply with the first step of the geofence protocol, therefore, Google must search across all LH journal entries to identify

users with potentially responsive LH data, and then run a computation against every set of coordinates to determine which LH records match the time and space parameters in the warrant.

After Google has completed that search, it assembles the LH information that is responsive to the request without any account-identifying information. This anonymized "production version" of the data includes an anonymized device number, the latitude/longitude coordinates and timestamp of the reported location information, the map's display radius,[8] and the source of the reported location information (that is, whether the location was generated via Wi-Fi, GPS, or a cell tower). The volume of data produced at this stage depends on the size and nature of the geographic area and length of time covered by the geofence request, which vary considerably from one request to another.[9]

Second, the government reviews the anonymized production version to identify the anonymized device numbers of interest. If additional anonymized location information for a specific device is necessary to eliminate false positives or otherwise determine whether that device is actually relevant to the investigation, law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request. Here, for example, the government requested a second round of anonymized LH information showing where certain users moved during an extended period of time 30 minutes

[8] Each set of coordinates saved to a user's LH includes a value, measured in meters, that reflects Google's confidence in the reported coordinates. A value of 100 meters, for example, reflects Google's estimation that the user is likely located within a 100-meter radius of the reported coordinates.

[9] *See, e.g.*, Jennifer Valentino-DeVries, N.Y. Times, *Tracking Phones, Google Is a Dragnet for the Police* (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html (discussing examples); Tony Webster, Minnesota Public Radio, *How Did The Police Know You Were Near A Crime Scene? Google Told Them* (Feb. 7, 2019), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants (same).

before and 30 minutes after the original timeframe. This additional contextual LH information can assist law enforcement in eliminating devices that were not in the target location for enough time to be of interest, were moving through the target location in a manner inconsistent with other evidence, or otherwise are not relevant to the investigation. The government then reviews users' movements, as reflected in the anonymized data, and selects the anonymized device numbers for which it will require Google to produce identifying user account information.

Third, the government can compel Google to provide account-identifying information for the anonymized device numbers that it determines are relevant to the investigation. Typically, the legal request requires Google to provide account subscriber information such as the Gmail address associated with the account and the first and last name entered by the user on the account.

The steps necessary to respond to a geofence request are thus quite different from and far more intrusive than responses to requests for CSLI or "tower dumps." To produce a particular user's CSLI, a cellular provider must search its records only for information concerning that particular user's mobile device. A tower dump is similarly limited: It requires a provider to produce only records of the mobile devices that connected to a particular cell tower at a particular time. But because Google LH information on a user's account is distinct from a mobile device's location-reporting feature, Google has no way to identify which of its users were present in the area of interest without searching the LH information stored by every Google user who has chosen to store that information with Google.

II. THE STORED COMMUNICATIONS ACT REQUIRES THE GOVERNMENT TO OBTAIN A WARRANT TO COMPEL PRODUCTION OF "LOCATION HISTORY" INFORMATION

Although the parties' briefing has focused on the Fourth Amendment, the Court's resolution of the important questions presented here should reflect the entire legal landscape.

Google's storage and disclosure of user data, including LH information, is subject to the SCA, which governs law-enforcement efforts to compel service providers such as Google to disclose data relating to a user's stored electronic communications. *See* 18 U.S.C. § 2703. The SCA generally requires the government to obtain a warrant supported by probable cause to require a provider to disclose the "contents" of electronic communications (such as the contents of an email). *Id.* § 2703(a), (b)(1)(A); *United States v. Graham*, 824 F.3d 421, 437 (4th Cir. 2016) (en banc), *overruled on other grounds*, 138 S. Ct. 2206.[10] By contrast, if the government uses legal process requiring a less demanding showing than probable cause—such as a court order or subpoena—it can generally only compel the production by a provider of basic subscriber information (using a subpoena) and other "records" of electronic communications, such as data indicating when an email was sent or to whom, but without the content of the email (using a court order). *See* 18 U.S.C. § 2703(c), (d).

[10] The SCA draws a distinction between government access to the contents of electronic communications in "electronic storage in an electronic communications system for one hundred and eighty days or less"—for which a warrant is invariably required—and access to the contents of electronic communications in "electronic storage in an electronic communications system for more than one hundred and eighty days" or contents of electronic communications "in a remote computing service," for which a warrant is required unless the government complies with certain notice procedures. 18 U.S.C. § 2703(a), (b). That distinction, which reflected the technical landscape prevailing at the time of the SCA's enactment in 1986, has largely fallen into disuse. The statutory provisions purporting to allow warrantless access to "contents" of communications under certain conditions without a warrant have been held unconstitutional, *see United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), and the Department of Justice has followed that holding as a matter of policy since 2013 by always using warrants to obtain stored content, *see* H.R. Rep. No. 114-528, at 9 (2016). In any event, Google acts as a provider of both an "electronic communication service" and a "remote computing service" in regard to LH information, and the information sought in this case was in storage for less than 180 days at the time of the warrant, rendering these statutory distinctions irrelevant in this case. *See In re Application of the United States of America for a Search Warrant for Contents of Elec. Mail and for an Order Directing a Provider of Elec. Comm'cn Servs. to not Disclose the Existence of the Search Warrant*, 665 F. Supp. 2d 1210, 1213 (D. Or. 2009) ("Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time … , rather than to define the service provider itself.").

Google LH information is subject to the SCA's warrant requirement because that information qualifies as "contents" of "electronic communications." The SCA defines an "electronic communication" as a "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). And it defines the "contents" of such a communication as "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8). A user's LH information qualifies as "contents" within that statutory definition. Google's users employ LH to record where they have been and when. In doing so, they "transfer" signals and data to Google, *id.* § 2510(12)—data that Google processes to fill users' Timelines and compile an accurate record of users' whereabouts, among other things. The user's location itself is the "substance" and "meaning" of the data the user transfers to Google, *id.* § 2510(8). The user's locations and movements are the "substance, purport, [and] meaning" of the data transmitted and they fill the digital journal that the Timeline feature provides. Although the contents of that journal are reflected on a map in one's Google account rather than in a written document, the locations and travels recorded therein are fundamentally the contents of the journal, capable of being reviewed, edited, and deleted by the user. Such information is plainly "contents" under the Act.

To be sure, location-reporting data in other contexts is sometimes considered to be "records" of electronic communications (sometimes called "metadata") because it is transmitted incidentally to a user's interaction with his or her mobile device. Sending such location data to a third party, in other words, is sometimes an ancillary byproduct of using a mobile device for other purposes (*e.g.*, to make a call or to find the best route home). That is certainly true of CSLI. As the Supreme Court explained in *Carpenter*, CSLI is generated "[e]ach time the phone

connects to a cell site," which can occur "several times a minute" in order to maintain the phone's function. 138 S. Ct. at 2211; *see also Graham*, 824 F.3d at 433 ("CSLI is non-content information because 'cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves.'"). As the Third Circuit has explained, however, location data need not be ancillary to an electronic communication; often, location data "serves no routing function, but instead comprises part of a communication's substance" itself. *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 136 (3d Cir. 2015). The question is whether the location information serves as "dialing, routing, addressing, or signaling information," or whether, as here, such information is "part of the substantive information conveyed to the recipient"—in which case "by definition it is 'content.'" *Id.*; *see also id.* at 137; *In re Certified Question of Law*, 858 F.3d 591, 594 (Foreign Int. Surv. Ct. Rev. 2016) (holding that digits an individual enters on a dial pad after dialing a telephone number, such as a PIN or a bank account number, qualify as content information because they transmit substantive information).[11] When users convey their locations to Google to save and store using the LH service, the data is not performing a "routing" or "addressing" role; it is itself the "substantive information" of the user's communications, 806 F.3d at 137, and thus "contents" for the purpose of the SCA.

Because LH information is "contents" under the SCA, the government must generally obtain a warrant to compel Google to disclose it—just as it would have to do to compel Google to produce the contents of a user's written journals stored on Google Drive. *See* 18 U.S.C.

[11] *See also* Orin Kerr, Volokh Conspiracy, Wash. Post, *Websurfing and the Wiretap Act* (June 4, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/ ("the line between contents and metadata is not abstract but contextual with respect to each communication").

§ 2703(a), (b)(1)(A); *Warshak*, 631 F.3d at 288. Thus, regardless of the Fourth Amendment analysis, the government was required to obtain a warrant in this case and to satisfy all the substantive and procedural obligations attending the issuance of a warrant.

III. ABSENT AN APPLICABLE EXCEPTION, THE FOURTH AMENDMENT REQUIRES THE GOVERNMENT TO OBTAIN A WARRANT TO COMPEL PRODUCTION OF "LOCATION HISTORY" INFORMATION

The Constitution also required a warrant in this case. 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. The Amendment's purpose "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Camara v. Municipal Court*, 387 U.S. 523, 528 (1967). The Fourth Amendment protects people against unreasonable "searches," and governmental action that intrudes upon an "expectation of privacy" that "society is prepared to recognize as 'reasonable'" constitutes a search. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Because the government's acquisition of Google LH information via a geofence request intrudes upon just such a reasonable expectation of privacy, it constitutes a search for which a warrant is generally required.

Under the traditional *Katz* analysis, Google's users have a reasonable expectation of privacy in their LH information. Google LH information "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'"—what the Supreme Court described in *Carpenter* as "the privacies of life." 138 S. Ct. at 2217 (quotation marks omitted). The Court in *Carpenter* held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured" through the government's acquisition of cell-site location information. *Id.* The same is true of Google LH information.

The question in *Carpenter* was "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." 138 S. Ct. at 2211. As the Supreme Court explained, access to such records implicates two lines of precedent: one addressing "a person's expectation of privacy in his physical location and movements" and the other "draw[ing] a line between what a person keeps to himself and what he shares with others." *Id.* at 2215-2216. The government's ability to obtain CSLI plainly implicated a person's "reasonable expectation of privacy in the whole of [his] physical movements." *Id.* at 2217. By obtaining historical location data generated by a person's cell phone, the Court explained, the government could obtain "an all-encompassing record of the holder's whereabouts," thus "revealing not only his particular movements" but the most intimate details of his or her life, *id.* at 2217-2218; *see also Riley v. California*, 573 U.S. 373, 403 (2014) ("With all [modern cell phones] contain and all they may reveal, they hold for many Americans 'the privacies of life.'"). And while it was true that cell-phone-generated location information was shared with a third party (the cellular provider), the Court reasoned, that did not diminish users' reasonable expectation of privacy in that information, given that it constituted—in essence—"a detailed chronicle of a person's physical presence compiled every day [and] every moment." *Carpenter*, 138 S. Ct. at 2220; *see also United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements…."); *United States v. Aigbekaen*, 943 F.3d 713, 723 (4th Cir. 2019) (referring to location history as "unusually sensitive").

The same factors that led the Court in *Carpenter* to find a reasonable expectation of privacy in historical CSLI apply just as forcefully to Google LH information. Google LH information, like the CSLI at issue in *Carpenter* and the GPS data in *Jones*, permits the

government to ascertain where a person has been and when—contravening the person's "legitimate expectation of privacy in the record of his physical movements." 138 S. Ct. at 2217. As was true of the CSLI at issue in *Carpenter*, by compelling Google to disclose LH information, the government can, "[w]ith just the click of a button," access a "deep repository of historical location information at practically no expense." *Id.* at 2218. Such data is remarkably revealing. Like CSLI, Google LH information lets the government "travel back in time to retrace a person's whereabouts." *Id.* In fact, the LH information at issue here is significantly more granular than the data at issue in *Carpenter*. The CSLI at issue there allowed the government to trace a suspect to an area that could have been as wide as four square miles. *Id.*; *see also id.* at 2232 (Kennedy, J., dissenting). By contrast, the information recorded in a Google user's LH information potentially records a person's whereabouts to within a matter of meters. *See supra* p. 10. The privacy interests implicated by Google LH information are thus even greater than in *Carpenter*.[12]

Here, the government argues—just as it did in *Carpenter*—that users have no reasonable expectation of privacy in their Google LH information because such records consist only of data that users have "revealed to a third party." Opp. 9. But the Supreme Court rejected that argument in *Carpenter*, and this Court should do the same here. The so-called third-party

[12] As noted, each individual estimate of a user's location reflected in the LH service has a margin of error, which distinguishes it from CSLI. *See supra* n.7. But that does not undermine the fact that a user has a reasonable expectation of privacy in her location as it is reflected in LH information—especially given that such information draws on data that can be far more precise than is CSLI and is highly reliable in context. At the same time, the margin of error associated with LH data means that the government's effort to use this information for purposes for which the LH service was not designed creates a likelihood that the LH data will produce false positives—that is, that it will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there. That, in turn, means that the potential incursion on privacy is quite significant indeed.

doctrine, as the Court explained in *Carpenter*, traces its roots to *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979)—cases in which the government obtained "business records" of a defendant's bank (in *Miller*) and telephone company (in *Smith*) that revealed personal information about the defendants. In each case, the Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," *Smith*, 442 U.S. at 743-744, and concluded that no search had occurred. But the Supreme Court in *Carpenter* conclusively rejected the argument that the doctrine should extend to CSLI. 138 S. Ct. at 2219-2220. For one, the Court explained, "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information" collected today by third parties of all kinds. *Id.* at 2219; *cf. United States v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007) (individuals have a reasonable expectation of privacy in the contents of their text messages). For another, the Court reasoned, "the second rationale underlying the third-party doctrine"—voluntary exposure—did not justify the application of the doctrine to CSLI, given that, for multiple reasons, users did not genuinely "share" such data with phone companies. *Carpenter*, 138 S. Ct. at 2220.

Neither of the two "rationale[s] underlying the third-party doctrine" justifies extending that doctrine to the LH information here. *Carpenter*, 138 S. Ct. at 2219-2220. First, it is not the case that Google users have a "reduced expectation of privacy" in LH information. *Id.* at 2219. As described above, LH functions in effect as a daily journal of a user's whereabouts and movements with a potentially high degree of precision. It can reveal when a user was at her home (or someone else's), a doctor's office, a place of worship, a political meeting, or other sensitive locations. The information is far more revealing than the bank records or telephone pen

register information at issue in *Smith* and *Miller*, and users expect that information to remain private. *See supra* pp. 6-10.

Second, as in *Carpenter*, the fact that users voluntarily choose to save and share LH information with Google does not on its own implicate the third-party doctrine, to the extent that doctrine is still viable. 138 S. Ct. at 2220.[13] The Court in *Carpenter* emphasized that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.* (quoting *Riley*, 573 U.S. at 385). For many users, the same is true of the location-based "services that [cell phones] provide," *id.*—including the ability to track one's own movements and enrich one's electronic footprint with that information. Moreover, unlike the business records of the third-party bank and telephone company in *Smith* and *Miller*, LH information is not compiled "for … business purposes" by the third party, *Smith*, 442 U.S. at 743—the key factor that justified the development of the doctrine in the first place. Rather, it is created and stored at the discretion of the user for the user's own purposes and remains in the user's control. Such relationships are common in the digital age. In *Warshak*, for instance, the fact that individuals transmitted their emails to a third party did not stop the court from finding that those individuals enjoyed a reasonable expectation of privacy in the contents of their emails. *See Warshak*, 631 F.3d at 288 (rejecting the applicability of the third-party doctrine and explaining that "the best analogy" was "cases in which a third party carries, transports, or stores property for another"—cases in which "the customer grants access to the [provider] because it is essential to the customer's interests"). The same is true here.

[13] *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (observing that the third party doctrine espoused by *Smith* and *Miller* is "ill suited to the digital age").

The government alternatively argues that *Carpenter* does not apply because the request here applied to a supposedly small area and a shorter period of time than the CSLI requests in *Carpenter*. Opp. 6-8. But there is nothing limited about a geofence search. As explained, *see supra* pp. 12-13, in order to conduct such a search, Google must search across the records of the account holders who entrust Google with their personal LH information. That is a significant incursion on privacy. Unlike the CSLI requests in *Carpenter*, moreover, which rested on the government's belief that particular suspects were involved in a crime—and which sought information only for those users—when the government seeks LH information via a geofence request, it does not know whose records it is searching for. The result is that the government obtains information associated not only with a specific person of interest whose actions might have given rise to probable cause or at least reasonable suspicion, but for numerous others who happened to have LH information from the area. The government's comparison to a "tower dump" (Opp. 8) fails for essentially the same reasons. A tower dump entails a search of records relating only to those mobile devices that were present in the defined area at the defined time; a geofence request requires a search across all Google users for their LH information. And a tower dump yields data that is significantly less granular than a user's LH.

Ultimately, although the time period covered by the warrant here is shorter than the CSLI requests in *Carpenter*, that distinction does not defeat Google's users' reasonable expectation of privacy. A shorter timeframe could make a dispositive difference when dealing with CSLI or tower dump information because a snapshot of such data, if sufficiently limited in duration, would not result in "a detailed and comprehensive record of the person's movements." *Carpenter*, 138 S. Ct. at 2217. It would reveal only that a particular device was at a particular place at one narrow point in time. But because of its greater granularity and precision, a Google

user's LH information allows the government to reconstruct a "detailed and comprehensive record of [the user's] movements," even if only for an hour or two—something that law enforcement would not be able to do using traditional investigative methods. *Id*. at 2217.

A request compelling production of Google LH information accordingly constitutes a search within the meaning of the Fourth Amendment. Unless an exception applies, the government thus "must generally obtain a warrant supported by probable cause before acquiring such records." *Carpenter*, 138 S. Ct. at 2221.

CONCLUSION

Google takes no position on whether the warrant in this case satisfies the requirements of probable cause and particularity or, if it does not, whether suppression is appropriate. But in resolving those questions, the Court should take into account the complete factual and legal context, and it should hold that both the SCA and the Fourth Amendment require the government to obtain a warrant to compel Google to search LH information via a geofence search. That result is compelled by the statute and the Constitution and the cases applying them. It is also the only result that takes appropriate account of the singularly broad and intrusive nature of a geofence search and the granularity of the intimate detail it produces. Given the capacity of geofence searches to intrude on personal privacy, their use should be supervised by a neutral magistrate and restricted to cases in which the government can establish probable cause.

Dated: December 20, 2019

Respectfully submitted,

/s/ Brittany Blueitt Amadi
Brittany Blueitt Amadi (Va. Bar No. 80078)
Catherine Carroll (Va. Bar. No. 50939; *pro hac vice* pending)
Alex Hemmer (*pro hac vice* pending)
WILMER CUTLER PICKERING HALE AND DORR LLP
1875 Pennsylvania Ave. NW
Washington, DC 20006
Tel: (202) 663-6000
Fax: (202) 663-6363
brittany.amadi@wilmerhale.com
catherine.carroll@wilmerhale.com
alex.hemmer@wilmerhale.com

Counsel for Amicus Google LLC