No. 25-112

IN THE
Supreme Court of the United States

OKELLO CHATRIE,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

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

JOINT APPENDIX
VOLUME I

D. JOHN SAUER
Counsel of Record
SOLICITOR GENERAL
UNITED STATES
DEPARTMENT OF JUSTICE
950 Pennsylvania Avenue, NW
Washington, DC 20530
(202) 514-2217
supremectbriefs@usdoj.gov

Counsel for United States

ADAM G. UNIKOWSKY
Counsel of Record
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
AUnikowsky@jenner.com

Counsel for Okello Chatrie

Petition for a Writ of Certiorari filed July 28, 2025
Certiorari Granted January 16, 2026

TABLE OF CONTENTS

Volume I

Volume II

Volume III
UNDER SEAL

NOTICE

The following documents have been omitted in the printing of this Appendix. They may be found in the Petitioner's Appendix at the following pages:

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

TABLE OF AUTHORITIES

STATUTES AND RULES

Fed. R. Crim. P.
17 ....[JA-11]
41 ....[JA-13]

OTHER AUTHORITIES

Google, Choose Which Apps Use Your Android Phone's Location, https://support.google.com/android/answer/6179507 (visited Dec. 20, 2019) ....[JA-17]

Google, Find And Improve Your Location's Accuracy, https://support.google.com/maps/answer/2839911 (visited Dec. 20, 2019) ....[JA-21]

Google, Manage Your Android Device's Location Settings, https://support.google.com/accounts/answer/3467281 (visited Dec. 20, 2019) ....[JA-17]

Google, Manage Your Location History, https://support.google.com/accounts/answer/3118687 (visited Dec. 20, 2019) ....[JA-17, 18]

H.R. Rep. No. 114-528 (2016)..................................[JA-28]

Kerr, Orin, Volokh Conspiracy, Wash. Post, Websurfing and the Wiretap Act, (June 4, 2015), https://www.washingtonpost.com/news/volokhconspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/ ....[JA-30]

Valentino-DeVries, Jennifer, 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 ....[JA-25]

Webster, Tony, 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..[JA-25]

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

[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.

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 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 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

[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).").

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.

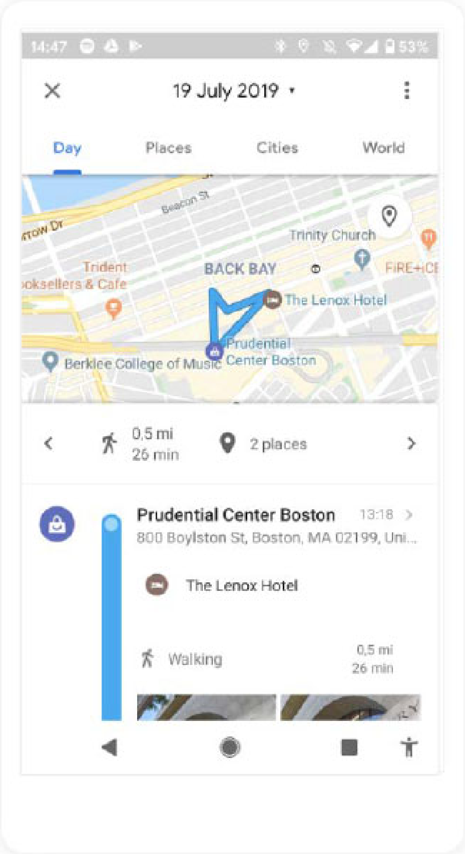


Figure 1. Sample Google Timeline.

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,

[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).

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 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

[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).

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 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

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

far more precise location information derived by triangulation between the phone and various satellites.”).[7]

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,

[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 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.

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 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

[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).

anonymized LH information showing where certain users moved during an extended period of time 30 minutes 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

[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

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 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).

Google LH information is subject to the SCA's warrant requirement because that information qualifies as "contents" of "electronic communications." The SCA

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.").

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

[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").

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. § 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

[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.

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 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,

[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").

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.

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

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

DECLARATION OF MARLO MCGRIFF

I, Marlo McGriff, respectfully submit this declaration in regard to the above-captioned matter. I make this declaration based on my knowledge of the facts stated herein.

1. I am a Location History Product Manager at Google, where my responsibilities include the Location History product. I joined Google in 2011 and have been in my current role since 2016.

2. I lead the cross-functional Location History team and am the overall Location History lead, setting the near-term goals and long-term strategy for the product.

I. Google Location History

3. Some Google services require a user to have a Google account before she can use the service at

all, like Gmail. Other services do not require a user to have an account, but offer additional functionality that is only available to Google account holders, like Maps and Search.

4. Google Location History ("LH") is a service that Google account holders may choose to use to keep track of locations they have visited while in possession of their compatible mobile devices. LH is not available to users who do not have a Google account. Users must explicitly opt in to the service.[14]

5. Google users can visualize their LH data through the "Timeline" feature of Google Maps, which operates as a journal that Google users can choose to use to create, edit, and store a record of their movements and travels. The Timeline feature processes the user's LH data to infer semantic location information such as place visits (*e.g.*, visit to a ski resort), activities (*e.g.*, driving), and paths between place visits (*e.g.*, driving from hotel to ski resort), which is then displayed to the user in her Timeline. LH and the Timeline feature thus allow a user to see where she has traveled with her device and when over a given period.

6. Users who opt into and use LH can access other benefits on their Google devices or applications as well. For instance, they can obtain personalized maps or recommendations based on places they have visited, get

[14] *See* Google, *Manage Your Location History*, https://support.google.com/accounts/answer/3118687?hl=en (visited Feb. 27, 2020).

help finding their phones, and receive real-time traffic updates about their commutes.

7. 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.[15] 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. Android users can also tailor their devices' location-reporting settings, controlling which sources of information (*e.g.*, GPS, cellular, or Wi-Fi) the device may use to determine location, and which applications can access location data. On iOS devices, the user must further configure her mobile device to share location information by granting the required device-level application location permission.

8. However, merely taking the steps described above—steps that are tied to a mobile device—does not on its own enable LH for a user's account. Google does not save LH information about where a particular mobile device has been to a user's account—even when the device-location feature is turned on and (for iOS) the required device-level application location permissions have been granted—

[15] *See generally id.*; Google Privacy & Terms, *How is location saved in my Google Account*?, https://policies.google.com/technologies/location-data#how-save (visited Feb. 27, 2020).

unless the user has also taken additional specific steps tied to her account.

9. For one, the user must opt into LH in her account settings and enable "Location Reporting"—a subsetting within LH—for each particular device on which she wants to use LH. 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. A single Google account can be associated with multiple devices, and the "Location Reporting" feature within LH allows users to select the specific devices on which they wish to enable LH.

10. 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 (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it.

11. When a user takes the above-mentioned steps, the resulting data is communicated to Google for processing and storage. Google stores this data in a database internally referred to as "Sensorvault." Only LH information is stored in Sensorvault.

12. LH information may be considerably more precise than other kinds of location data, including cell-site location information ("CSLI"). 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 could include 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, Bluetooth beacons, or cell towers. Combined, these inputs (when the user enables them) can be capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI. For example, I understand that when a strong GPS signal is available, a device's location can be estimated within approximately twenty meters or less.

13. In 2019, the majority of Google users worldwide did not have LH enabled on their account. While a more precise percentage is difficult to calculate in part due to fluctuating numbers of users, in 2019, roughly one-third of active Google users (i.e., numerous tens of millions of Google users) had LH enabled on their accounts.

14. Depending on a user's ads personalization setting, Google may use the semantic location information described in Paragraph 5 above (*e.g.*, place visits) that the Timeline feature infers from LH to show relevant ads to the user. For example, a user who regularly frequents ski resorts may later see an ad for ski equipment when watching a video on YouTube. Additionally, Google may also use the semantic location information that the Timeline feature infers from LH in an anonymized and aggregated manner to help advertisers measure how often an online ad campaign helps drive traffic to physical stores or properties. Google does not share LH or any other information

identifying individual users with advertisers.[16] Additionally, at all times relevant to this warrant, Google has not shared identified LH data with third parties except through legal process and has not monetized identified LH data.

15. Critically, as described in Google's Privacy Policy at https://policies.google.com/technologies/retention, a user remains in control of her LH data through her Timeline. She can review, edit, or delete her Timeline at will. By deleting Timeline entries, a user also deletes the underlying LH information. As such, the user could decide to keep LH information only for certain dates; she could delete all LH information except those associated with certain Timeline entries; she could instruct Google to automatically delete all LH information after a set period; or she could keep all LH information for future reference. When a user deletes data in her Google account, Google immediately starts the process of removing it from the product and our systems as described in Google's Privacy Policy, at https://policies.google.com/technologies/retention.

16. Google users may also opt into a separate service called Web & App Activity ("WAA"). If a user turns on the WAA setting in his or her Google account with the necessary app-level and device-level permissions (*e.g.*, if the device-location setting on the mobile device is active), some activities that the user engages in while logged into her account (for instance,

[16] *See* Google Privacy & Terms, *How is location used to show ads?*, https://policies.google.com/technologies/location-data#show-ads (visited Feb. 27, 2020).

Google searches) are saved to that account, so the user may have a more personalized experience. For example, she may experience faster searches and more helpful app and content recommendations, such as when a user sees her search automatically suggested based on past searches.[17] Some of these WAA entries can include location information, although the source of the location information will vary depending on the activity, the device, and the user's other settings. LH and WAA are separate services that store data in separate databases, and there are no dependencies between LH and WAA. WAA data is not used to calculate the locations that are stored in LH, and completing a search across LH data does not search or draw on WAA data in any way.

17. Google Location Accuracy ("GLA") is a separate setting, which was formerly known as Google Location Services. It is available only on Android mobile devices. When the GLA setting is turned off, an Android device will use only GPS data to calculate its location. If a user has the GLA setting on, the Android's location services will use additional inputs, including Wi-Fi access points, mobile networks, and sensors, to estimate the device's location.[18] While location data may be

[17] *See, e.g.*, Google, *See & control your Web & App Activity*, https://support.google.com/websearch/answer/54068?co=GENIE.Platform%3DAndroid&hl=en (visited Feb. 27, 2020); Google Privacy & Terms, *How is location saved in my Google Account?, at Web & App Activity*, https://policies.google.com/technologies/location-data#how-save (visited Feb. 27, 2020).

[18] *See, e.g.*, Google, *Manage your Android device's location settings*, https://support.google.com/nexus/answer/3467281?hl=en (visited Feb. 27, 2020).

periodically collected from devices with the GLA setting turned on and used in an anonymous way to improve location accuracy (*e.g.*, estimating the locations of WiFi access points and cell towers), that location data is not stored with user identifiers and is stored separately from the LH database and the WAA database.[19] As indicated, if a user has turned on GLA, then the device's location information that is sent to and stored in LH (if LH has been enabled) may be calculated using not only GPS-sourced data, but also WiFi- or cell-sourced data from the GLA database. In other words, GLA data might be used by the device to calculate a location data point that is then stored in LH. But there are no other dependencies between GLA and LH. Completing a search across LH data does not search or draw on GLA data in any way—the databases are separate and do not interact beyond the initial location calculation.

18. When GLA is turned on, the inputs used to calculate a user's estimated location can include WiFi access points. However, Google cannot reconstruct which WiFi access points were used to calculate a given LH data point. Although Google collects anonymized data in GLA that allows it to estimate the physical location of particular WiFi access points, and those WiFi access points in turn can be an input used to calculate a device's estimated location that is then stored in LH, Google does not know and cannot recreate which particular WiFi access points were used to calculate any particular LH data point. Google therefore cannot

[19] *See, e.g.*, Google Privacy & Terms, *How does Google know my location?*, at Google Location Services, https://policies.google.com/technologies/location-data (visited Feb. 27, 2020).

identify the physical location of the WiFi access points used to estimate a user's location coordinates stored in LH because it cannot determine which WiFi access points were used to estimate the user's location.

II. Google's Production of LH Information to Law Enforcement

19. I understand that this case concerns a so-called "geofence" request, which seeks LH information for all Google users whose LH information indicates that their device may have been present in a specified geographic area during a certain window of time.

20. In practice, LH is the only form of location data Google maintains that Google believes to be responsive to a geofence request, and LH is the only form of location data that was produced to the government in this case. This is because at all times relevant to this case, Google has not stored any other location information in association with specific Google user accounts that is sufficiently granular to be responsive to and searchable for such a request. To be relevant and responsive to a geofence warrant, location data must be stored in association with a specific user's account and must be able to pinpoint a user's estimated location with enough precision to bring it within the radius described in a geofence warrant. Even though Google devices and applications might sometimes use or transmit information about a user's location to Google while the device or application is in use, no such information other than LH is stored and searchable in association with specific user accounts at a level of

precision sufficient to be searched and produced in response to a geofence warrant.

21. At all times relevant to this case, WAA did not store a user's location at a level of detail precise enough to be responsive to a geofence warrant. Stored WAA data reflects a device's location to an approximate area of at least one square kilometer; and, if there are fewer than 1000 users in one square kilometer, the area is even larger. WAA data was therefore too coarse to be responsive to the warrant in this case and was not searched or produced.

22. Google does not store GLA data in association with any particular Google account. GLA data therefore is not responsive to a typical geofence warrant and was not responsive or relevant to the warrant in this case and was not searched or produced.

23. LH information can be searched in response to a geofence request. To conduct that search, Google must search across *all* LH data to identify users with LH data during the relevant timeframe, and run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant. Google does not know which users may have such saved LH data before conducting the search and running the computations.

24. The location data points reflected in LH are estimates based on multiple inputs, and therefore a user's actual location does not necessarily align perfectly with any one isolated LH data point. Each set of coordinates saved to a user's LH includes a value,

measured in meters, that reflects Google's confidence in the saved 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 saved coordinates based on a goal to generate a location radius that accurately captures roughly 68% of users. In other words, if a user opens Google Maps and looks at the blue dot indicating Google's estimate of his or her location, Google's goal is that there will be an estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot.

25. Notwithstanding the confidence interval described above, if a user's estimated location (*i.e.*, the stored coordinates in LH) falls within the radius of the geofence request, then Google treats that user as falling within the scope of the request, even if the shaded circle defined by the 68% confidence interval falls partly outside the radius of the geofence request. As a result, it is possible that when Google is compelled to return data in response to a geofence request, some of the users whose locations are estimated to be within the radius described in the warrant (and whose data is therefore included in a data production) were in fact located outside the radius. To provide information about that, Google includes in the production to the government a radius (expressed as a value in meters) around a user's estimated location that shows the range of location points around the stored LH coordinates that are believed to contain, with 68% probability, the user's actual location.

26. In contrast, the purposes for which Google designed LH do not depend on any individual stored LH

data points. For instance, the Timeline feature combines and contextualizes numerous individual stored LH data points over periods of time into inferred semantic location information (*e.g.*, place visits) so that users may store and visualize their location and movements in a journal (*e.g.*, visiting a hotel, visiting a ski resort, and driving between that hotel and ski resort). Similarly, Google may use such inferred semantic place visits (not individual stored LH data points) for ads. LH is sufficiently precise and reliable for these purposes for which Google designed LH.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 11th day of March 2020, in San Francisco.

/s/ Marlo McGriff
Marlo McGriff

This is an archived version of our Privacy Policy. View the current version or all past versions.

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

Effective May 25, 2018 | Archived versions | Download PDF

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for key terms. And if you have any questions about this Privacy Policy, you can contact us.

INFORMATION GOOGLE COLLECTS

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

Things you create or provide to us

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads

- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

You can visit your Google Account to find and manage activity information that's saved in your account.

Go to Google Account

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- IP address
- Sensor data from your device
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to save and manage your location information in your account.

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

WHY GOOGLE COLLECTS DATA

We use data to build better services

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, Security Checkup provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.

Go to Ad Settings

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

YOUR PRIVACY CONTROLS

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the Privacy Checkup, which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our Product Privacy Guide.

Go to Privacy Checkup

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your Google Account includes:

Privacy controls

Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.

Go to Activity Controls

Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

Go to Ad Settings

About you

Control what others see about you across Google services.

Go to About You

Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

Go to Shared Endorsements

Information you share

Control whom you share information with through your account on Google+.

Go to Information You Share

Ways to review & update your information

My Activity

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

Go to My Activity

Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

Go to Dashboard

Your personal information

Manage your contact information, such as your name, email, and phone number.

Go to Personal Info

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: Choose whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your YouTube Search History and your YouTube Watch History.
- Ad Settings: Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

You can also request to remove content from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

And finally, Inactive Account Manager allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a cookie in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services rely on cookies to function properly, for things like remembering your language preferences.
- Device-level settings: Your device may have controls that determine what information we collect. For example, you can modify location settings on your Android device.

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private.

Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing a song in Play, your name and photo appear next to your activity. We may also display this information in ads depending on your Shared endorsements setting.

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you use Google Home to request a ride from a ride-sharing service, we'll get your permission before sharing your address with that service. We'll ask for your explicit consent to share any sensitive personal information.

With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite), your domain administrator and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our Transparency Report.
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

KEEPING YOUR INFORMATION SECURE

We build security into our services to protect your information

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like Safe Browsing, Security Checkup, and 2 Step Verification to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may

be disciplined or terminated if they fail to meet these obligations.

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.

Export your data

To delete your information, you can:

- Delete your content from specific Google services
- Search for and then delete specific items from your account using My Activity
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account

Delete your information

In some cases, we retain data for limited periods when it needs to be kept for legitimate business or legal purposes. You can read about Google's data retention periods, including how long it takes us to delete your information.

We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain servers around the world and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

ABOUT THIS POLICY

When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to archived versions for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

RELATED PRIVACY PRACTICES

Specific Google services

The following privacy notices provide additional information about some Google services:

- Chrome & the Chrome Operating System
- Play Books
- Payments
- Fiber
- Project Fi
- G Suite for Education
- YouTube Kids
- Google Accounts Managed with Family Link

Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- Your Google Account is home to many of the settings you can use to manage your account
- Privacy Checkup guides you through key privacy settings for your Google Account
- Google's safety center offers advice for staying safe & secure
- Google's privacy site provides more information about how we keep your information private and safe

- Privacy & Terms provides more context regarding this Privacy Policy and our Terms of Service

- Technologies and Principles includes more information about:

    - How Google uses cookies

    - Technologies used for Advertising

    - How Google uses pattern recognition to recognize things like faces in photos

    - A page that explains what data is shared with Google when you visit websites that use our advertising, analytics and social products.

    - How Google uses data when you use our partners' sites or apps

ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." Learn more about Google ads and why you may see particular ads.

the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you contact most frequently.

phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. Learn more

payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. Learn more

devices

For example, we can use information from your devices to help you decide which device you'd like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features.

Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. Learn more

services to make and receive calls or send and receive messages

Examples of these services include:

- Google Hangouts, for making domestic and international calls
- Google Voice, for making calls, sending text messages, and managing voicemail
- Project Fi, for a phone plan

Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. Learn more

publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate.

protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account

- Photos and videos you upload to Google Photos are used to help you create albums, animations, and other creations that you can share. Learn more
- A flight confirmation email you receive may be used to create a "check-in" button that appears in your Gmail

ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it's taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can learn more here. You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can search and browse privately or turn off signed-out search personalization.

personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. Learn more

sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services.

may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. Learn more

safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.
- The “last account activity” feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. Learn more

detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

combine the information we collect

Some examples of how we combine the information we collect include:

- When you're signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. Learn more
- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. Learn more
- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about

your interests, like sports scores, based your activity. Learn more

- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. Learn more

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

Learn more about how Google uses data when you use our partners' sites or apps.

partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. Learn more

specific Google services

For example, you can delete your blog from Blogger or a Google Site you own from Google Sites. You can also delete reviews you've left on apps, games, and other content in the Play Store.

rely on cookies to function properly

For example, we use a cookie called 'lbcs' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. Learn more

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our Transparency Report.

show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. Learn more

specific partners

For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. Learn more about these partners and how they use your information.

servers around the world

For example, we operate data centers located around the world to help keep our products continuously available for users.

third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

appropriate safeguards

For example, we may anonymize data, or encrypt data to ensure it can't be linked to other information about you. Learn more

ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

Customizing our services

For example, we may display a Google Doodle on the Search homepage to celebrate an event specific to your country.

Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. Learn more about the companies providing business services in the EU.

Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

Cookies and similar technologies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.

Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for "cars" looks like this:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 -
740674ce2123e969
```

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.

- 25/Mar/2003 10:15:32 is the date and time of the query.
- http://www.google.com/search?q=cars is the requested URL, including the search query.
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.
- 740674ce2123a969 is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

Unique identifiers

A unique identifier is a string of characters that can be used to uniquely identify a browser, app, or device. Different identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed.

Unique identifiers can be used for various purposes, including security and fraud detection, syncing services such as your email inbox, remembering your preferences, and providing personalized advertising. For example, unique identifiers stored in cookies help sites display content in your browser in your preferred language. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. Learn more about how Google uses cookies.

On other platforms besides browsers, unique identifiers are used to recognize a specific device or app on that device. For example, a unique identifier such as the Advertising ID is used to provide relevant advertising on Android devices, and can be managed in your device's settings. Unique identifiers may also be incorporated into a device by its manufacturer (sometimes called a universally unique ID or UUID), such as the IMEI-number of a mobile phone. For example, a device's unique identifier can be used to customize our service to your device or analyze device issues related to our services.

GOVERNMENT
EXHIBIT
3b
3:19CR130

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

SUPPLEMENTAL DECLARATION OF MARLO MCGRIFF

I, Marlo McGriff, respectfully submit this declaration in regard to the above-captioned matter to supplement my prior declaration, filed on March 11, 2020. ECF No. 96-1. I make this declaration based on my knowledge of the facts stated herein.

1. I reviewed the testimony of Spencer McInvaille, Mr. Chatrie's advisory witness, ECF No. 81 ("McInvaille Testimony"), and the video exhibit Mr. McInvaille presented as Exhibit 4 during the January 21, 2020 hearing as to Mr. Chatrie's Motion for Discovery Regarding the Government's Use of Google's Sensorvault Data ("McInvaille Video").

2. As explained in my prior declaration, enabling the Location History ("LH") service requires a Google user to take multiple steps. ECF No. 96-1 at 2.

3. One of those steps, as referenced at ECF No. 96-1 at Paragraph 9, is that the user must opt in to LH in her account settings. LH is disabled in account settings by default, and LH remains disabled unless and until the user enables it.

4. Until recently, a user could enable LH in her account settings during account creation, which can occur during device setup. An example of this is depicted in the McInvaille Video (at 2:50-3:17) and the McInvaille Testimony (at 50-52). During his testimony, Mr. McInvaille did not enable LH during account creation. *See* McInvaille Testimony at 51-52, 53.

5. A user may also enable LH in her account settings through an app that has LH-powered features, such as the Google Maps app. An example of this is partially depicted in the McInvaille Video (at 4:38-4:45) and the McInvaille Testimony (at 55-57). During his testimony, Mr. McInvaille opened the Google Maps app and was shown a screen stating "Get the most from Google Maps" with two choices: "YES, I'M IN" or "SKIP" as depicted in the last screen at the end of the McInvaille Video (at 4:45); *see* McInvaille Testimony at 56-57.

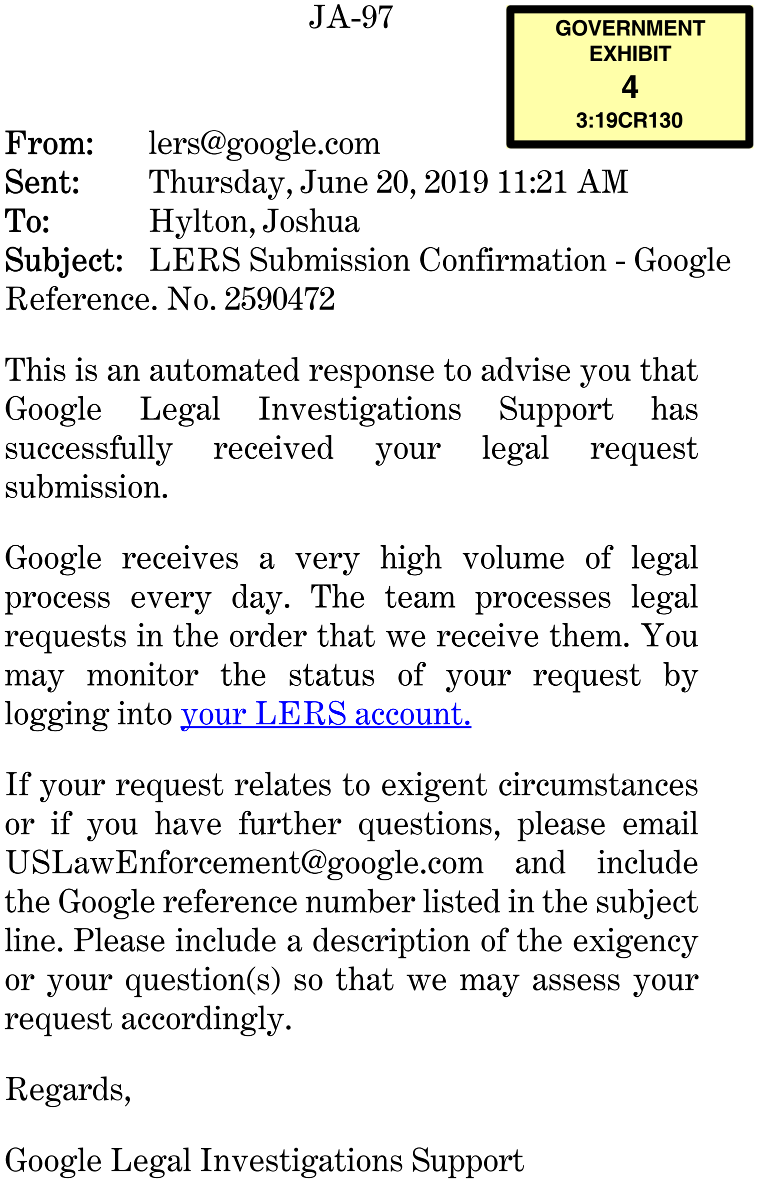
6. The McInvaille Video ended at that step, without depicting what would happen if the user tapped on "YES, I'M IN." McInvaille Video at 4:45 (stopping at the "Get the most out of Google Maps" screen).

7. By 2017 at the latest, it was not possible for a user to enable LH solely by tapping on "YES, I'M IN" as depicted on the final screen in the McInvaille Video. Instead, a user who tapped on "YES, I'M IN" when prompted would be presented with a second opt-in screen. Only by opting in via that second screen could the user successfully enable LH for her account. Sensorvault rejects LH opt-ins from unsupported flows or devices. Accordingly, Sensorvault would have rejected any attempted opt-in through the manner described by Mr. McInvaille, and LH would not have been successfully enabled.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 12th day of June 2020, in San Francisco.

/s/ Marlo McGriff
Marlo McGriff



GOVERNMENT EXHIBIT
4
3:19CR130

From: lers@google.com
Sent: Thursday, June 20, 2019 11:21 AM
To: Hylton, Joshua
Subject: LERS Submission Confirmation - Google Reference. No. 2590472

This is an automated response to advise you that Google Legal Investigations Support has successfully received your legal request submission.

Google receives a very high volume of legal process every day. The team processes legal requests in the order that we receive them. You may monitor the status of your request by logging into your LERS account.

If your request relates to exigent circumstances or if you have further questions, please email USLawEnforcement@google.com and include the Google reference number listed in the subject line. Please include a description of the exigency or your question(s) so that we may assess your request accordingly.

Regards,

Google Legal Investigations Support

From: Hylton, Joshua [redacted]
Sent: Tuesday, June 25, 2019 3:00 PM
To: USLawEnforcement@google.com
Subject: 2590472

Expedition request based on armed and dangerous subject(s) still at large. Subject was on cell phone just prior to violent act; therefore, Google may have captured pertinent information to identify and arrest parties involved.

Respectfully,

Master Detective J.P. Hylton Unit: 936 Criminal Investigations Division: Persons Unit

[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: lers@google.com
To: Hylton, Joshua
Subject: Production For Google Reference Number 2590472 Is Available for Download
Date: Friday, June 28, 2019 6:01:43 PM

Your production -- Google Reference Number 2590472 -- is now available for download. Please visit LERS and click on the files link to view all available files.

The download links will expire in 14 days. If you are unable to download your production within this window, contact USLawEnforcement@google.com with your Google Reference Number and we will reinstate the files so long as we still maintain a copy of the files.

If you have questions about your production, please contact USLawEnforcement@google.com with your Google Reference Number in the subject line.

Regards,

Google Legal Investigations Support

From: Hylton, Joshua [redacted]
Sent: Monday, July 01, 2019 4:40 PM
To: USLawEnforcement@google.com
Cc: Simon, Kenneth (USAVAE)
Subject: Google Ref. No. 2590472

Google Legal Team,

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936 Criminal Investigations Division: Persons Unit

[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua [redacted]
Sent: Tuesday, July 02, 2019 9:54 AM
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668
10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936 Criminal Investigations Division: Persons Unit

[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936 Criminal Investigations Division: Persons Unit

[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua [redacted]
Sent: Monday, July 08, 2019 9:33 AM
To: USLawEnforcement@google.com
Subject: 2590472
Importance: High

Google Legal Team,

I'm writing to inquire about my correspondence with your office on 07/01 and 07/02. Please keep in mind that expedition is requested based on armed and dangerous subject(s) still being at large. Subject was on cell phone just prior to violent act; therefore, Google may have captured pertinent information to identify and arrest parties involved. See below:

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959

12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936

Criminal Investigations Division: Persons Unit

[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua [redacted]
Sent: Tuesday, July 09, 2019 10:37 AM
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

As discussed yesterday over the phone, I appreciate your quick response and willingness to provide GPS data for the below device ID(s). Please expedite this request where possible due to this suspect's continued threat to our community. If it would speed up the process, please provide data as it becomes accessible/available, starting with device ID(s) 1 – 9. It was mentioned that the larger the request, the more time it will take to get data back. With this in mind, I will still have to rule out device ID(s) 1-9; however, I may be able to do so more quickly if I can begin reviewing data. The faster I can review the data, the faster I can get this guy/guys off the street.

Thanks again for your professionalism and understanding. I realize that I'm asking for a lot and you and your team are likely tasked-out already, but any and all assistance and expedited process is MUCH appreciated.

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662

9. 1207269668

If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936

Criminal Investigations Division: Persons Unit

[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936 Criminal Investigations Division: Persons Unit

[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: lers@google.com
Sent: Tuesday, July 09, 2019 10:25 PM
To: Hylton, Joshua
Subject: Production For Google Reference Number 2590472 Is Available for Download

Your production -- Google Reference Number 2590472 -- is now available for download. Please visit LERS and click on the files link to view all available files.

The download links will expire in 14 days. If you are unable to download your production within this window, contact USLawEnforcement@google.com with your Google Reference Number and we will reinstate the files so long as we still maintain a copy of the files.

If you have questions about your production, please contact USLawEnforcement@google.com with your Google Reference Number in the subject line.

Regards,

Google Legal Investigations Support

From: Hylton, Joshua [redacted]
Sent: Wednesday, July 10, 2019 1:40 PM
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

Thank you guys for the extremely quick turnaround on the Stage Two data. After plotting the nine device ID(s) with additional geographical data, I have narrowed my search for subscriber info to three device ID(s):

1.) **1716665659**
2.) 907512662
3.) -1662304683

Please send me the subscriber information for the above device ID(s) as soon as possible. The involved offender is still a threat to the community and may be a flight risk as well. Again, I can’t thank the Google Legal team enough for your professionalism, quick response, and understanding in the captioned matter.

If you have any questions or concerns, please don’t hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit

[redacted]

“If you only do what you can do, you will never be better than what you are now.”

From: Hylton, Joshua [redacted]
Sent: Thursday, July 11, 2019 9:24 AM
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

Thank you guys for the extremely quick turnaround on Stage(s) One and Two. I'm emailing to inquire about yesterday's request (07/10) for the below device ID(s)' subscriber information. The United States Attorney's Office is waiting for that return before moving forward with additional search warrants.

1.) **1716665659**
2.) 907512662
3.) -1662304683

Please send me what you can as soon as possible. The involved offender is still a threat to the community and is a likely flight risk. Again, I can't thank the Google Legal team enough for your professionalism, quick response, and understanding in the captioned matter.

If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: lers@google.com
Sent: Thursday, July 11, 2019 7:21 PM
To: Hylton, Joshua
Subject: Production For Google Reference Number 2590472 Is Available for Download

Your production -- Google Reference Number 2590472 -- is now available for download. Please visit LERS and click on the files link to view all available files.

The download links will expire in 14 days. If you are unable to download your production within this window, contact USLawEnforcement@google.com with your Google Reference Number and we will reinstate the files so long as we still maintain a copy of the files.

If you have questions about your production, please contact USLawEnforcement@google.com with your Google Reference Number in the subject line.

Regards,

Google Legal Investigations Support

From: Hylton, Joshua [redacted]
Sent: Friday, July 12, 2019 11:37 AM
To: USLawEnforcement@google.com
Cc: Simon, Kenneth (USAVAE)
Subject: 2590472

Google Legal Team,

Thank you guys for getting back with me regarding the subscriber information included with my Stage Three returns. While reviewing data for all three accounts, I could not locate any associated telephone numbers for the following Google account and ID:

- Okellochatrie55@gmail.com
- Google Account ID: 365520819283

Please include any such data, as the following is listed in my search warrant:

"After review and upon request by Law Enforcement, Google Inc. shall provide identifying account information/CSI for the accounts requested by Law Enforcement. This identifying account information/CSI **shall include all of the following that are available:** user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, **electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used t set up the account, verify the account or to receive assistance**

with the account, and Google Voice phone numbers associated with the account."

Please let me know what you find, as soon as possible, as the offender involved is still a threat to the community and may be a flight risk as well. I will CC Assistant United States Attorney, Kenneth Simon, for tracking purposes or follow-up questions.

If you have any concerns, please don't hesitate to call,

[redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit

[redacted]

"If you only do what you can do, you will never be better than what you are now."

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

UNITED STATES OF AMERICA	Criminal No. 3:19CR130
v.	March 5, 2021
OKELLO T. CHATRIE	

DAY TWO

COMPLETE TRANSCRIPT OF MOTION TO SUPPRESS BEFORE THE HONORABLE M. HANNAH LAUCK UNITED STATES DISTRICT JUDGE

****

[Page 536]

D'ERRICO – DIRECT

****

BY MR. SIMON:

****

Q Now, did you also -- we've talked about Phase 1. What happens in the second stage of the warrant? How does that work?

A The second stage of the warrant is where Detective Hylton sent to Google a list of device IDs that were identified as being relevant to the investigation for [Page 537] additional location data for those device IDs.

And that would include, I believe, 30 minutes prior and 30 minutes following the original geofence time frame with no restraints on location, so that we can see the path of travel for these devices.

Q Is that the -- what we heard Sarah Rodriguez refer to as sort of the second stage, being that contextual Location History information?

A That's correct. It provides context for us so that if there is somebody that is just driving by, we try to eliminate them if we can. If there is somebody that is in another parking lot, still within the geofence and not in the area, we try to eliminate them, if we can, or we may need more additional information to evaluate them as a suspect and either eliminate or include them as a suspect.

Q Now, did you do the same thing that you did at the first stage with those second round records in terms of summarizing what we got back?

A Yes, I did.

Q All right. Looking at Slide 26, is this the -- are these the summaries of those records?

A These are. It summarizes the nine device IDs that we obtained records for from Google in Stage 2.

Q And it looks like the number of records this time [Page 538] is a bit larger. We've got more records; right?

A That's correct. This time we received 680 records.

Q Okay. And if we look at the far right, there is a smallest maps display radius and a largest maps display radius. Describe those.

A That' s correct. So, similar to how I analyzed the Stage 1 data, I also looked at the size of the display radiuses for the Stage 2 data. And those columns reflect the smallest display radius for that device and the largest display radius for each device.

Q And how many of those records in the second stage belong to the defendant' s account?

A The defendant, again, device ID 1716665659, the second line from the bottom. We received 94 records for the defendant' s device.

Q And this is a second stage that gives that additional 30 minutes on each side of the time, but also has no regard for -- at this point we're outside of the geofence now; right?

A That' s correct. We can see the path of travel for each of these devices or if they were stationary for this time, we could see that as well. But it does not have the geographical constraints of being immediately in the area of the bank robbery. [Page 539]

Q And these second stage records, to the extent we get them, that's after a discussion generally between law enforcement, maybe the prosecutor and others involved; right?

A Correct. We evaluate each of the devices and determine if this device could be a witness to the crime, could be a suspect to the crime, could be an accomplice. We evaluate each of them to make a determination.

Q And what, if anything, goes into consideration of -- and particularly in this case, was there any consideration of the need to not only inculpate somebody, sort of inculpatory evidence, but exculpatory evidence?

A Absolutely. We would like to exclude as many people as possible. And we can use the second stage to do that, to make sure that we're looking at the person that's actually responsible for committing this crime.

Q Okay. In looking at Slides 27 and 28 -- I'm sorry, 28 and 29, are these the plotting of the defendant's records at Stage 2 ?

A Yes. So Slide 28 shows the complete records for the defendant in Stage 2 from about 3:50 p.m. through 5:50 p.m. [Page 540]

Q All right. Let's look at the left side here. Maybe we'll just bring it up by itself, Slide 28.

Can you walk us through the numbers here? Is this going in sequential order, the one through seven boxes here?

A Yes. So the first records we received are on the top of the page, the bubble to the right. The box is marked with a No. 1. There's two records in that area, both with the exact same latitude and longitude, the exact same center point. And those points are at 3:53:10 p.m. and 3:55:20 p.m.

The first point is 104 meters. And then we see that second point expand to nearly 1800 meters, which, again, is indicative to me of travel.

Then we see the device show up on -- towards the top left of the slide illustrated by Box 2 with a similar situation, 3:57:23 p.m. and 3:59: 32 p.m., two records with the exact same center points, exact same latitude and longitude, the first one with a smaller display radius of 92 meters, and the second one with a larger display radius of over 1700 meters. Again, indicative of travel.

Q In looking at those two points, just to make sure we're talking about this right, this is prior to the robbery; right? [Page 541]

A Yes, it is.

Q And so these, again, are records at the second stage that are going to give us more context about where folks are moving?

A That' s correct.

Q In looking at now -- you went through one and two. The third box here, can you go through those?

A Excuse me. Which boxes?

Q The third box of records on Slide 28.

A Yes. The third box contains the records in the immediate vicinity. Just about all the records for the geofence. And those are records for the time of 4:01 p.m. to 4:54 p.m. And those records are in that immediate vicinity of the Call Federal Credit Union and Journey Christian Church.

Q And so this is 54 of the records that we got at the second stage? I'm sorry. These are records that would be in both stages; right?

A Correct. Box 3 are records that would be -- not all -- I don't believe all of them are in the second stage, but most of them are. They're in that area.

Q Then you can -- can you walk us through what else we have here?

A Yes. Box No. 4 illustrates a GPS trail. So when I map these records, I think it's important to denote [Page 542] the source of the record. So my red points are going to be GPS-based records and my blue points are going to be Wi-Fi-based records.

So we can see a trail in rapid succession more detail than we see anywhere else on this map of points from 4:58 p.m. to 5:04 p.m. with very small display radiuses of 3 meters to 10 meters leading away from the area of the bank robbery, down towards the area of 288, which is the road that traverses west to east on the bottom of the map.

Q Okay. Now, did you ultimately look at some sort of final records from this supplemental return?

A I did. Records 5, 6, and 7, those blocks, illustrate travel back towards the Mason Dale Drive area with the box with No. 7, the 18 Wi-Fi records, being in that immediate area of Mason Dale Drive.

Q In looking at Slide 29, is this the area of Mason Dale?

A Yes, it is. I've drawn all of the Wi-Fi points and the display radiuses on the map, as well as I tried to point out every residence that is either touched or in the area of those locations provided by Google.

Q What residence, ultimately, did Detective Hylton conclude, based on additional investigation, belonged [Page 543] to the defendant?

A The address was 4702 Mason Dale Drive. The box is the second box down on the right side, which points pretty much to the center of the screen.

Q Now, using any of these particular Wi-Fi points, is it apparent exactly which house is hitting these Wi-Fi points?

A No. These records are not clear enough for me to say go get a search warrant to arrest or conduct a search of a house in this area. Additional investigative steps are needed in order to refine this data and determine where this device actually was located at this time.

Q Okay. And so this is -- this is the full extent of the second stage that we see here?

A That' s correct, yes.

Q Okay. Now, looking at Slides 31 and 32, what happens at the third stage of the warrant?

A The third stage is where we go to Google again, and we submit to them the device IDs of which we want subscriber information for those device IDs. We requested three device IDs. And Google provided four things. They provided a file that maps the device ID that was in our geofence warrant to the account's Google ID. And based off that Google ID, they [Page 544] provided the subscriber information for that account. And that's because that device ID is not a unique identifier across the entire Google-sphere. It is only a unique identifier within an account and within this geofence.

Q In looking at, on the right side, at Slide 32, is that the precise subscriber information we got for this defendant's device at the third stage?

A That' s correct. So up top there' s the table of the GAIA ID, which is the Google ID with the device ID that we mentioned before being associated with the defendant, 1716665659. We can see that that associated Google ID is listed in the subscriber information file that is on the lower part of the page, which is associated with the account that contains the name Jamaican Media with an email address of okellochatrie55@gmail.com.

Q Okay. Does it appear, the created on date there? There's a line that says "created on" on the right side on Slide 32. What is that?

A Yes. Three lines above the highlighted Google account ID there is a created on date, which indicates that this account was created on August 20, 2017 at 6:04 p.m. UTC.

Q And between August 2017 and July 2018, according [Page 545] to Google records, Location History wasn't enabled on the relevant device; right?

A Can you repeat that question?

Q Well, let me ask it this way, because I think you have some facts about this. When the phone that the defendant enabled Location History on, the Samsung Galaxy S9 , do you have a sense of when that phone came to market?

A I do. I believe --

Q It' s Slide 38 .

A Yes. It came to market on March 16, 2018, which is several months after the date of the creation date for this Google account.

Q Okay. And I think that my question that was going to be there, I'll just scratch that from the record. It wasn't to the point.

Now, with respect to the third round of information that we got on the three IDs, did you ultimately plot the points for the other two devices that we requested subscriber information on?

A Yes, I did.

Q Okay. Let' s look at the device that ends in 2662 and Slides 33 and 34.

A Slide 33 indicates the one point that we received back, the one record of Location History that we [Page 546] received in Stage 1 for device 907512662. And that plots a center point over the Journey Christian Church at about 4:35 p.m., prior to the time of the bank robbery.

Q Okay. And so why go back at the second stage here?

A Well, there are several reasons. So, the first reason is this is a device that was present in the area of the bank prior to the bank robbery. And we know that sometimes when people want to hide their location, they'll turn their phones off. And if their phone is turned off, no additional Location History would be reported for that device. So it's significant to us that there is a point inside the geofence that occurred prior to the bank robbery with no points after the bank robbery. Because we also believe that after a subject has robbed a bank, that they are going to flee the area and not be -- or not have any additional Location History records within this geofence several minutes after the bank robbery.

Q And, now, what about on the right side? Are we seeing the second stage records after we've requested the second stage on this device?

A That' s correct. This is a plot of the second stage records which travel a bit in the area. The [Page 547] first record that we have is 4:35 p.m. in the vicinity of the Journey Christian Church, and that's towards the top of the page with a call out box on the right side. That is the same point that we saw in the last slide.

The next reference point on the slide is travel towards the south ending up near box No. 2 where there are records at 4:47 and 4:53 p.m.

After this box, the phone retraces some of its steps north and then ends up near the apartment complex just south of the Call Federal Credit Union in Boxes 3 and 4. And to me, this is indicative of a trail of somebody that could have dropped off somebody in the parking lot, traveled a ways, and then returned to possibly pick up somebody that traveled through the woods between the Call Federal Credit Union and the apartment complex directly south of that area.

Q Okay. And there was a third device that we saw subscriber information on; correct?

A That' s correct. That was device - 1662304683.

Q And you plotted those points on Slides 35 and 36?

A Yes, I did.

Q All right. Now, tell us, when we pull those up on 35 and 36, what we see in Slide 35 at Stage 1 inside the geofence and why go back at Stage 2 and get [Page 548] supplemental records on this particular record?

A Yes. These initial records that we received in Phase 1 shows us three Wi-Fi points. Two of the center points are directly on top of the Call Federal Credit Union and one location point is towards the right that covers the area of the Journey Christian Church. These points are between 4:44 and 4: 47 p.m. And for the same reasons that I discussed prior, we know that subjects may turn off their phone to avoid transmitting Location History or device or being observed on the cellular network to obscure their location.

So with this device having points before and no points after, we thought this was -- we needed additional records to be able to see the context of this travel.

Q What about the second stage? Is that on the right side?

A Yes, Slide 36 provides that context of travel for us. And the first record we see is towards the center of the screen. There is a cluster of points marked by box No. 1 at 4:39 p.m.

There's another cluster of points that traveled northeast on Hull Street towards box No. 2, which is the area of the Call Federal Credit Union and the [Page 549] Journey Christian Church. And those records are there at 4:44 through 4:47 p.m.

And then we see the phone travel back east -- I'm sorry -- travel west on Hull Street Road or appearing to be traveling -- appearing to be near Hull Street Road marked with box No. 3 at 4:55.

This becomes interesting to us because we see somebody that starts away from the bank, moves towards the bank, and then immediately leaves that area, which could indicate that they are dropping somebody off at that bank.

Q Now, just let me end with a question going back to Slides 23 and 24. We've talked about the investigation in this case and, in particular, I'm looking at the defendant's plot points on 23 and 24 when they come up. Did you and Detective Hylton reach a conclusion about whether this was the account, just based on Stage 1, that belonged to the person who robbed the Call Federal Credit Union on May 20, 2019?

A Based on several pieces of evidence, including witness testimony that indicated there was a suspicious blue Buick parked behind the church, which is notated on Slide 24 with the green box in the area where the red GPS points are clustered, combined with the video observations from the Journey Christian [Page 550] Church and the Call Federal Credit Union, and the description of the individual and the visual of the individual, we determined that this was likely the device that belonged to -- that most resembled the device that would belong to the subject of the bank robbery.

Q And this is based merely off of the returns that came at the first stage that called for Google to only return devices that it determined were inside that geofence radius at the time of the crime; correct?

A That's correct. That is relying solely on that Stage 1 data without evaluating any of the contextual data that we received at Stage 2.

MR. SIMON: No further questions, Judge.

****