GEOFENCE WARRANTS: THE NEW BOUNDARIES

Ronald J. Rychlak[*]

INTRODUCTION

A geofence is a virtual perimeter that surrounds or defines an identified geographic area. Sensors along the boundary of the area can detect the presence of electronic communication devices on either side. Geofences have many uses, including, for instance, marketing and advertising aimed at potential customers in a

[*] Distinguished University Professor and Jamie L. Whitten Chair in Law and Government at the University of Mississippi. B.A. 1980, Wabash College; Distinguished Professoer of Law, Jamie L. Whitten Chair of Law and Government. J.D. 1983, Vanderbilt University School of Law. Ron has received the university's highest research and publication recognition, the "Distinguished Research and Creative Achievement Award" and the University's highest award in honor of service, the Algernon Sydney Sullivan Award. For thirteen years, Ron served as the law school's Associate Dean for Academic Affairs, and since 2007 he has served as the university's Faculty Athletic Representative and chair of the University's Athletics Committee.

geographic area or establishing areas from which online sports bets may legally be made.[1]

Customers of Google (and certain other online providers) can enable their devices so that the providers can track usage of their services over time and maintain records of when devices were located in various geographic areas.[2] According to 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 [(Location History)] 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.[3]

Of course, since this collected data is recorded, a geofence can be created after the fact,[4] and Google can determine which devices were within a certain area at any given time.[5]

---

[1] *How Google Uses Location Information*, GOOGLE: PRIVACY & TERMS, https://policies.google.com/technologies/location-data?hl=en-US [https://perma.cc/3744-CU4A] (last visited Apr. 3, 2023); Larry Henry, *Geofencing Technology Limiting Wagering to Within State Boundaries Works Well, Tech Expert Says*, GAMBLING.COM, https://www.gambling.com/us/news/geofencing-technology-works-expert-says-2927500 [https://perma.cc/2JDS-74ZL] (last updated Sep. 28, 2022). "Since Google started collecting [and storing this data] in 2009, [its] advertisement revenue has increased almost tenfold." *Google Data and Geofence Warrant Process*, NAT'L LITITG. SUPPORT BLOG F (June 6, 2022), https://nlsblog.org/2022/06/06/google-data-and-geofence-warrant-process-2/ [https://perma.cc/A7M2-PJAA].

[2] Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant at 6, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) [hereinafter Brief of Amicus Curiae].

[3] *Id.* at 6 ("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.").

[4] *See Id.* at 5 ("[Location History] allows those users to keep track of locations they have visited while in possession of their mobile devices.").

[5] A. Reed McLeod, *Geofence Warrants: Geolocating the Fourth Amendment*, 30 WM. & MARY BILL RTS. J. 531, 548 (2021) ("Google has begun to take steps to automatically delete location data, [but] that near perfect record is stored by default for eighteen months on Google servers.").

Increasingly, location data is being requested by the government in the form of geofence warrants.[6] Such warrants seek to identify all cell phone users whose data suggests they were in a certain area in a given timeframe.[7] Geofence warrants are used in situations where traditional warrants would not be effective. For example, if law enforcement agencies are investigating a crime but have no witnesses, geofence data can provide valuable information about a suspect's movements and whereabouts.[8] Such data can also be used to determine who was located at the scene of an incident.[9] "[T]he information retrieved in response to a geofence warrant is pervasive, detailed, revealing, retroactive, and cheap."[10]

The location data that is usually requested in geofence warrants, Google LH information, differs in significant respects from the type of data that courts have considered in other Fourth

---

[6] Brief of Amicus Curiae, *supra* note 2, at 3 ("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.").

[7] *In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 732 (E.D. Ill. 2020) ("The idea behind a geofence warrant is to cast a virtual net–in the form of the geofence – around a particular location for a particular time frame."). Perhaps a more descriptive name would be a reverse location history search warrant. McLeod, *supra* note 4, at 534. Such warrants have been called a "novel but rapidly growing technique." Brief of Amicus Curiae, *supra* note 2, at 3. Google reported that it had received 982 such warrants in 2018, 8,396 in 2019, and 11,554 in 2020. Johana Bhuiyan, *The New Wwarrant: How US Police Mine Google for Your Location and Search History*, THE GUARDIAN (Sep. 16, 2021) https://www.theguardian.com/us-news/2021/sep/16/geofence-warrants-reverse-search-warrants-police-google [https://perma.cc/37RU-YWPS].

[8] McLeod, *supra* note 4, at 536 ("It seems unmistakable that this investigative tool holds great potential for solving complex crimes that would otherwise never be solved.").

[9] Mark Lanterman, *Geofence warrants: The battle is just beginning,* MINNESOTA STATE BAR ASS'N (Feb. 26, 2023), https://www.mnbar.org/resources/publications/bench-bar/columns/2021/04/05/geofence-warrants-the-battle-is-just-beginning [https://perma.cc/2SFF-XYSC] (last visited Apr. 3, 2023) (using such data to identify people who entered the U.S. Capitol building on January 6, 2021); Bonnie Kristian, *Geofencing Warrants Are a Threat to Privacy*, REASON FOUND. (Dec. 5, 2022, 11:00 AM), https://reason.com/2022/12/05/geofencing-warrants-are-a-threat-to-privacy/ [https://perma.cc/D87L-XGRT].

[10] Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2510 (2021). They are less expensive and require far less manpower than other means of investigation to obtain similar evidence.

Amendment cell phone cases, such as *Carpenter v. United States*.[11] For one thing,

> "Google LH information can be considerably more precise than other kinds of location data [. . .][.] That is because" LH location-reporting relies "not only [on] information related to the locations of nearby cell sites, but also on 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.[12]

Combined, these inputs (when the user enables location tracking) are capable of estimating a device's location to a high

---

[11] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (considering CSLI data) ("Whether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements . . . ."); United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). *See also* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 227-30 (2018). The Libertas Institute, which questions the constitutionality of geofence warrants, has identified three types:

> (1) searches requesting data from cell towers servicing a specific location, on a certain day, for a set period of time (generally a few hours); (2) searches requesting data that "pinged" to a tower within a specific radius (e.g., a few hundred meters); and (3) searches requesting data from the Google Reverse Location database. This type of warrant does not list a specific physical area for the search, instead relying on Google's ID numbers to serve as digital markers.

Geofence "Warrants": An Unconstitutional Abuse of Technology, LIBERTAS INST., https://libertas.org/wp-content/uploads/2022/08/memo-geofence.pdf [https://perma.cc/7J5P-37YE] (last visited April 7, 2023) (noting that these three types of searches may be combined by law enforcement). Only the first of the three, however, actually describes a geofence situation; moreover, that description is incomplete. *Id.*

[12] Brief of Amicus Curiae, *supra* note 2, at 10.

degree of precision.[13] For example, when a strong GPS signal is available, a device's location can be estimated within approximately twenty meters."[14] That is far more accurate than the cell site location information (CSLI) data that was evaluated in *Carpenter*.[15]

Another significant difference between geofence data and CSLI data relates to the scope of the surveillance. In *Carpenter*, authorities sought information related to the suspect's phone, wherever it might have been, over the course of 127 days.[16] A

---

[13] It is more precise than either CSLI or GPS data. *See* Brief of Amicus Curiae, *supra* note 2, at 10.

> A smartphone device with a Google account, data services on, and Location History enabled will transmit the location of that device based on multiple different inputs: "GPS and Bluetooth signals, Wi-Fi connections, [] cellular networks" all provide a reading on the phone, as well as internal sensors like "accelerometer[s] and barometer sensors, . . . gyrometer and magnetometer sensors . . . ." Reporting indicates that this layering of multiple inputs provides location tracking of a device accurate "to within a few yards" and with a pattern that is updated "in some cases . . . more than 14,000 times a day."

McLeod, *supra* note 4, at 538-39 (footnotes omitted) (alterations in original). "Google has also attested to the accuracy of its location data, and that it is significantly more precise than the location data considered in *Carpenter*." *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning Arson Investigation, 497 F. Supp. 3d 345, 360 (N.D. Ill. 2020). *But cf.* Kristian, *supra* note 8 ("That map is not certain to be accurate; it does not prove that the phone's owner was the one making those movements; and even with complete accuracy and certainty, there's no guarantee police will interpret the map correctly.").

[14] Brief of Amicus Curiae, *supra* note 2, at 10. *See also Find and Improve Your Location's Accuracy*, GOOGLE: GOOGLE MAPS HELP, https://support.google.com/maps/answer/2839911?hl=en&co=GENIE.Platform%3DAndroid# [https://perma.cc/Q95H-UEXM] (last visited Mar. 10, 2023). *But see* Brief of Amicus Curiae, *supra* note 2, at 10 (citing *Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting) ("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."); United States v. Beverly, 943 F.3d 225, 230 n.2 (5th Cir. 2019) ("CSLI should not be confused with GPS data, which is far more precise location information derived by triangulation between the phone and various satellites.").

[15] "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)." Brief of Amicus Curiae, *supra* note 2, at 8-9 (citing *Carpenter*, 138 S. Ct. at 2211-12). *See also* Freiwald & Smith, *supra* note 10, at 227-30.

[16] *Carpenter*, 138 S. Ct. at 2212.

typical geofence warrant requests information related to the location of cell phones within a restricted area over the course of just a few hours.[17]

Of course, this science has not been employed without controversy. Privacy advocates argue that geofence warrants violate the rights of innocent individuals who happen to have been near the scene of a crime or other places that they would prefer to keep private.[18] Their location can be monitored "even though law enforcement has no particularized basis to suspect that [they] played a role in, or possess any information relevant to, the crime being investigated."[19] The advocates also argue that the process effectively involves *all* cell phones that have Location History enabled.[20]

This paper will argue that geofence data is a valuable tool for law enforcement and that most privacy objections are not well founded. However, the process commonly employed to obtain data involves obtaining a warrant at the wrong time. A change in timing of the warrant application process will better protect citizens from actual invasions of privacy.

I. BACKGORUND ON GEOFENCE WARRANTS

Geofence warrants, also known as "reverse location" or "geographic" warrants, allow law enforcement agencies to obtain information about all devices within a specific geographic area at a particular time. This information can include location data, IP

---

[17] Brief of Amicus Curiae, *supra* note 2, at 12.

[18] *Geofence "Warrants": An Unconstitutional Abuse of Technology*, *supra* note 10 (noting that these three types of searches may be combined by law enforcement). *See* Charlotte Scott, *Geofence Warrants Are 'Slippery Slope' in Texas*, SPECTRUM NEWS 1 (JULY 20, 2022, 8:48 PM), https://spectrumlocalnews.com/tx/south-texas-el-paso/politics/2022/07/21/geofence-warrants-are—slippery-slope—in-texas [https://perma.cc/SUT8-LC4Z] ("In a post-Roe Texas, anyone who provides an abortion can now face criminal penalties. . . . This month, Google announced its systems would automatically delete location data if someone visited a medical facility such as an abortion clinic or fertility center."); Zack Whittaker, *A Bill to Ban Geofence and Keyword Search Warrants in New York Gains Traction*, TECHCRUNCH (Jan. 13, 2022, 9:02 AM), https://techcrunch.com/2022/01/13/new-york-geofence-keyword-search-warrants-bill/ [https://perma.cc/Q8F4-YVWQ] (discussing a New York bill that would ban the use of geofence warrants statewide).

[19] Brief of Amicus Curiae, *supra* note 2, at 3.

[20] *See infra* notes 66-70 and accompanying text.

addresses, and other identifying information. "Geofence warrants rely on the vast trove of location data that Google collects from Android users — approximately 131.2 million Americans — and anyone who visits a Google-based application or website from their phone, including Calendar, Chrome, Drive, Gmail, Maps, and YouTube, among others."[21]

Requests for such warrants typically identify a geographic area surrounding a point of interest, such as a crime scene. This can, of course, include private homes and other sensitive locations. "A geofence request seeks to compel [the provider (usually Google)] to produce LH information for all [cell phone] 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."[22] The volume of data produced 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.[23]

The earliest geofence data requests tried to imitate "tower dump' requests" by seeking records of the mobile devices that connected to a particular cell tower at a particular time.[24] In light

---

[21] Note, *Geofence Warrants and the Fourth Amendment*, *supra* note 9, at 2512 (footnotes omitted). The number of Android OS phone users using Google's Location History services 133.4 million in 2022. *Number of Android Smartphone Users in the United States from 2014 to 2022*, STATISTA (Feb. 1, 2021), https://www.statista.com/statistics/232786/forecast-of-android-users-in-the-us/ [https://perma.cc/8EWK-TDXG].

[22] Brief of Amicus Curiae, *supra* note 2, at 12.

[23] *See, e.g.,* Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/H9K6-CQ74] (discussing examples); Tony Webster, *How Did the Police Know You Were Near a Crime Scene? Google Told Them*, MINNESOTA PUB. RADIO (Feb. 7, 2019, 3:10 PM), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants [https://perma.cc/D598-ZQ64].

[24] Brief of Amicus Curiae, *supra* note 2, at 12; 9-14 ("A tower dump . . . 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."). A tower dump includes "information on all the devices that connected to a particular cell site during a particular interval." Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

of the significant differences between CSLI and Google LH data, however, Google developed a three-step anonymization protocol to protect the privacy of its users, which has been incoporated into many warrant applications.[25]

A recent case out of Mississippi set forth a three-step process to obtain information sought from Google.[26] First, Google would first provide agents with a list of Google accounts found within the "box" during the specified time frame, with the devices only identified by an anonymous numerical identifier, without any content concerning the user of the device.[27] Step Two is for those accounts that the agents determined to be relevant to the investigation, Google would provide additional location history outside of the "box" to determine path of travel. This additional location information would not exceed 60 minutes either side of the first and last timestamp associated with the account in the initial dataset.[28] Finally, at Step Three, for those accounts deemed relevant following Step Two, Google would provide subscriber information to the agents.[29]

---

[25] "The three stage warrant process is based on an agreement between Google and the Department of Justice's Computer Crime and Intellectual Property Section . . . ." *Google Data and Geofence Warrant Process*, *supra* note 1.

[26] *See* United States v. Smith, No. 3:21-cr-107-SA, 2023 WL 1930747 (N.D. Miss. Feb. 10, 2023).

[27] *Id.* at *2 ("The first step requires Google to search its Sensorvault for *all* users who have location history enabled at the time the warrant was executed.").

[28] *Id.*

[29] *Id.* at *3; *see also Brief of Amicus Curiae*, *supra* note 2, at 11. According to at least one commentator, "in practice it appears that law enforcement routinely skips Stage Two and moves directly from Stage One to Stage Three analysis." *Google Data and Geofence Warrant Process*, *supra* note 1. *See also In re Matter of the Search Warrant Application for Geofence Location Data Stored at Google Concerning Arson Investigation*, 497 F. Supp.3d at 345, 353 (N.D. Ill. 2020) (refering to a two-step process).

The most significant privacy questions about geofence warrants relate to Step Three, but most warrants are obtained prior to Step One.[30] That should change.

A warrant at Step One compels 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 certain geographic area during a defined timeframe. The issue identified by privacy advocates is that Google has no way to know in advance which users have LH data indicating their presence in particular areas at particular times.[31] So, in order to comply with the request, Google must search across all LH journal entries and then run a computation against every set of coordinates to determine which LH records match the time and space parameters in the warrant.[32] Advocates point out that this means searches are being conducted of people about whom there is no probable cause, reasonable suspicion, or even a mere hunch.[33]

II. PRIVACY ISSUES

Geofence warrants obtained at Step One authorize searches of location history databases, based on the chance that someone

---

[30] *See e.g.* United States v. Chatrie, 590 F. Supp. 3d 901, 916 (E.D. Va. 2022); *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 747 (N.D. Ill. 2020); *In re* Information Stored at Premises Controlled by Google, 2020 WL 5491763, at *6 (N.D. Ill. 2020). Step Two is not significantly involved in the warrant analysis process. In United States v. Carpenter, No. 8:21-cr-309-VMC-MRM, 2023 WL 3352249, at *5 (M.D. Fla. 2023), the defense had an expert testify during the Suppression hearing. He said that he most commonly sees a three-step process, but in this case, it was a two-step process. *Id.* at *6, *8. The first step included Google searching its Location History, and the second step involved getting the subscriber information. *Id.* at *6.

[31] *See* Brief of Amicus Curiae, *supra* note 2, at 7 ("Not all mobile applications can use location inofrmation, and . . . will do so only if the user configures her device to allow the app to use the mobile device's location information.").

[32] *See Id.* at 6.

[33] *See Geofence Warrants and the Fourth Amendment*, *supra* note 9, at 2514 ("[G]eofence warrants are usually sealed by judges. While some explain this practice by pointing to the Stored Communications Act, its text merely requires 'a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction.' The Act does not mention sealing, and the government has conceded there are no 'default sealing or nondisclosure provisions.' . . . This secrecy prevents the public from knowing how judges consider these warrants and whether courts have been consistent, increasing the need for not only transparency but also uniformity in applying the Fourth Amendment to geofence warrants." (footnotes omitted)).

connected to the crime might be identified.[34] Such warrants routinely involve the collection of data pertaining to innocent people who were in the area at the time of the crime, and privacy advocates argue that this constitutes a search.[35]

> [R]ather 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.[36]

The privacy issues raised at this stage, however, are similar to those encountered by individuals who have their fingerprints or DNA samples included in a larger pool against which new evidence is compared. In none of these cases are the individuals exposed to invasive searches or in any other way invaded or restricted.[37] From a police perspective, it is similar to interviewing witnesses or reviewing surveillance video. The more serious privacy issues arise in Step Three.

A. The Fourth Amendment

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[38] In *Katz v. United States*, the U.S. Supreme Court described the Fourth Amendment as a protection of people, not places, and said that what a person "seeks to preserve as private,

---

[34] *Id.* at 2515.

[35] *See, e.g., id.* at 2509 (explaining how an innocent bike rider in Gainesville, Florida, and another innocent man were identified as suspects by geofencing). "While all geofence warrants provide a search radius and time period, they otherwise vary greatly. Some, for example, will expand the search area by asking for devices located '*outside* the search parameters but within a margin of error.'" *Id.* at 2514.

[36] Brief of Amicus Curiae, *supra* note 2, at 3-4.

[37] *See generally* Ronald J. Rychlak, *DNA Fingerprinting, Genetic Information, and Privacy Interests,* 48 TEXAS TECH L. REV. 245, 246 (2015); Ronald J. Rychlak, *Genetic Information and Privacy Interests: The DNA Fingerprinting Act,* 8 ENGAGE: J. OF FEDERALIST SOC'Y PRAC. GRPS. 64 (2007).

[38] U.S. CONST. amend. IV.

even in an area accessible to the public, may be constitutionally protected."[39] A government intrusion into a person's private sphere qualifies as a "search," triggering the Fourth Amendment's requirement that the intrusion be authorized by a warrant supported by probable cause.[40] The Supreme Court also has recognized that an intrusion need not be "trespassory" to be considered a search for Fourth Amendment purposes.[41]

In *Carpenter v. United States*, the Supreme Court spoke of a cell phone holder's "anticipation of privacy in his physical location."[42] Such 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 Court described as "the privacies of life."[43] "[A]n individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [the government's acquisition of] CSLI."[44]

The question for the Court 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."[45] The answer was yes; CSLI data implicated a person's "reasonable expectation of privacy in the whole of [his] physical movements."[46] The Court explained that with historical location data generated by a person's cell phone, the government could obtain "an all-encompassing record of the holder's whereabouts," thus "revealing

---

[39] 389 U.S. 347, 351-52 (1967).

[40] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

[41] *See* United States v. Jones, 565 U.S. 400, 412-13 (2012) (affirming court of appeals decision that required a warrant for a search that tracked an individual's movements for twenty-eight days with global positioning technology).

[42] *Carpenter*, 138 S. Ct. at 2217 ("As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" (quoting Jones v. California, 565 U.S. 400, 415 (2012))).

[43] *Id.* (quotation marks omitted).

[44] *Id.*

[45] *Id.* at 2211. "[T]he location data in a geofence warrant can provide the same 'intimate window into a person's life' for the same long periods of time that concerned the Court in [*Carpenter*]." McLeod, *supra* note 4, at 548 (quoting Justice Roberts in *Carpenter*).

[46] *Carpenter*, 138 S. Ct. at 2217.

not only his particular movements," but the most intimate details of his or her life.[47]

The differences between CSLI data and Step One Google LH information are that the geographic information identified with a geofence warrant, though it may be more precise, does not relate to the user's "particular movements,"[48] because the particular user remains unknown. It also does not extend over a significant time frame. In *Carpenter*, the authorities compiled information about the location of the defendant's phone over 127 days.[49] Google LH information obtained in Step One typically involves anonymized data spread over just a few hours. It does not provide the "intimate

---

[47] *Id.* at 2217-18; *see also Riley*, 573 U.S. at 403 ("With all [modern cell phones] contain and all they may reveal, they hold for many Americans 'the privacies of life.'"). In *Riley*, the Court held that a search warrant is required to conduct a search, incident to arrest, of the contents of a suspect's cellular telephone. *Riley*, 573 U.S. at 401.

> *Riley* based its holding in large part on a recognition that given the large amount of data that some electronic devices can store, their owners have a reasonable expectation of privacy with respect to the contents:
>
> "Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom. Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.

In re Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 735 (N.D. Ill. 2020) (quoting *Riley*, 573 U.S. at 393). "The Court . . . held that a warrant is generally required to search the information on a cell phone . . . but did not go so far as to hold that the Fourth Amendment protects the use or location of a cell phone in real time." United States v. Ellis, 270 F. Supp. 3d 1134, 1142 (N.D. Cal. 2017).

[48] *Carpenter*, 138 S. Ct. at 2217-18.

[49] *Id.* at 2217.

window" into personal matters that concerned the Court in *Carpenter*.[50]

B. The Voluntary Nature of Location Data

"Location data" or "Location History" is an opt-in feature,[51] maintained by Google through either its own Android operating system or through cell phones using a Google service or application such as Gmail, Search and Maps.[52]

> 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.[53]

Location History is not a device-based setting; it is an account-level setting which Google uses to collect data across any device using the Google account.[54] Purposes of collecting Location History include enhancing user experience and targeting advertising.[55]

> Location History data serves Google's advertising business by providing "store visit conversions" or "ads measurement" to businesses based on user location. Without identifying any individual user, this "store conversion" data can follow a particular ad campaign and identify "how many users who saw a particular ad

---

[50] *Id. See also* Jones v. California, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

[51] Brief of Amicus Curiae, *supra* note 2, at 9.

[52] *See* Ryan Nakashima, *Google Tracks Your Movements, Like It or Not*, ASSOCIATED PRESS (Aug. 13, 2018, 5:15 PM), https://apnews.com/article/828aefab64d4411bac257a07c1af0ecb [https://perma.cc/D7T8-6958] (last visited March 16, 2023).

[53] Brief of Amicus Curiae, *supra* note 2, at 9.

[54] *See Manage Your Location History*, GOOGLE ACCT. HELP, https://support.google.com/accounts/answer/3118687?hl=en [https://perma.cc/7HDJ-XV2J] ("Location History is a Google Account setting that creates Timeline, a personal map that helps you remember[.]").

[55] *See How does Google use location information?*, GOOGLE PRIV. & TERMS, https://policies.google.com/technologies/location-data?hl=en-US [https://perma.cc/FH28-JE6Q] ("Google may use or save location information to provide people with useful services when they interact with Google products, such as providing locally relevant and faster search results, traffic predictions for people's daily commutes[.]").

> campaign actually went to one of those stores." Google's "radius targeting" also allows—again without identifying any user—"a business to target ads to users that are within a certain distance of that business."
>
> ***
>
> Indeed, Location History even allows Google to "estimat[e] . . . where a device is in terms of elevation." . . . [T]his capability helps locate someone in an emergency, or try to "determine if you are on the second [or first] floor of the mall" if the Google Maps directory has launched to help a user navigate indoors.[56]

Google collects the information associated with each account "in a repository called '*Sensorvault'*, which 'assigns each device a unique device ID . . . and stores all Location History data [for] use[] in . . .marketing."[57] *Sensorvault* is used in advertisement marketing and many other purposes, including depicting on Google Maps whether a certain location is busy during particular hours.[58]

For Google LH to function and save information about a user's location, however, the user must take several steps.[59] First, the user must ensure that the device-location setting on the phone is turned on. Second, the user must configure the device to share

---

[56] United States v. Chatrie, 590 F. Supp. 3d 901, 908 (E.D. Va. 2022) (first and third alteration in original). "Google's Location History provides users with enhanced functionality for the free Google Maps application and others." McLeod, *supra* note 4, at 538.

[57] *Google Data and Geofence Warrant Process*, *supra* note 1.

[58] *Chatrie*, 590 F. Supp. 3d, at 908.

[59] Amicus Briefing has stated:

> "[R]ather 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."

Brief of Amicus Curiae Google LLC in Support of Neither Party, *supra* note 2, at 3.

location information with applications capable of using that information.[60]

Even taking these steps does not generate a saved LH record of a Google user's locations. Google does not save information about where a particular mobile device has been unless the user has also taken additional steps tied to the Google account. Specifically, the user must opt into LH in the account settings and enable "Location Reporting" for the particular device. For the LH data to be kept, the user must also sign into the Google account on the device.[61]

Even after taking all of those steps, "[t]he user can review, edit, or delete his or her Timeline and LH information from Google's servers at will."[62]

The argument, of course, is that "users . . . opt in with less than explicit notice, or even with good notice" but do not understand "the potential consequences to their privacy if they opt in."[63] As one scholar has asked, "is it possible to participate in modern life without opting into Google location services?"[64] The answer is that "Google's Privacy Policy informs users about their data, how to keep it safe, and how to take control. And Google regularly publishes transparency reports that reflect the volume of requests for disclosure of user data that Google receives from government entities."[65]

---

[60] "Not all mobile applications can use location information, and those that can, such as Google Maps, will do so only if the user configures her device to allow the app to use the mobile device's location information." *Id.* at 7.

[61] *See* Privacy Policy, GOOGLE, https://policies.google.com/privacy/archive/20190122 [https://perma.cc/V6KS-JGSZ] (last visited Feb. 18, 2024). There are several reasons why you may want location services enabled on your phone. They include improved navigation based upon the user's current location, geotagging in social media apps to let followers see where the user is visiting, helping emergency responders quickly locate the user, and personalized content such as local weather forecasts or recommendations for nearby restaurants and such. *See* Jon Knight, *6 Reasons You Might Actually Want to Give Google Your Location Data*, GADGET HACKS (MAR. 27, 2018, 8:17 PM), https://smartphones.gadgethacks.com/how-to/6-reasons-you-might-actually-want-give-google-your-location-data-0183740/ [https://perma.cc/2S6H-SDFZ].

[62] *Id.* at 8. According to at least one account, Google's location history database is "notoriously difficult to opt out of." Libertas Institute, *supra* note 10.

[63] McLeod, *supra* note 4, at 543.

[64] Orin Kerr, *The Fourth Amendment and Geofence Warrants: A Critical Look at United States v. Chatrie*, LAWFARE INST. (Mar. 12, 2022, 3:34 PM), https://www.lawfareblog.com/fourth-amendment-and-geofence-warrants-critical-look-united-states-v-chatrie [https://perma.cc/7ML2-BP9Y].

[65] *Brief of Amicus Curiae*, *supra* note 2, at 1.

User control makes Google LH data significantly different from "the CSLI at issue in *Carpenter* or cellular data obtained via a 'tower dump.'"[66] "Mobile device users cannot opt out of the collection of CSLI or similar records, nor can they retrieve, edit, or delete CSLI data."[67] Therefore, Google LH users do not have the same expectation of privacy, nor do they experience the kind of privacy invasion the Court considered in *Carpenter*.[68]

C. The Third-Party Doctrine and Step One Warrants

In *Carpenter*, the Court considered the third-party doctrine, which holds that when information is shared with a third party, such as the cellular company, claims of privacy are waived.[69] In that case, the Court found that the third-party doctrine did not diminish the users' reasonable expectation of privacy because the information involved essentially constituted "a detailed chronicle of

---

[66] *Id.* at 8. "Wireless carriers collect and store CSLI [records] for their own business purposes, [such as identifying] weak spots in the[] network" or determining when to "apply[] 'roaming' charges." Carpenter v. United States, 138 S.Ct. 2206, 2212 (2018). "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." *Brief of Amicus Curiae*, *supra* note 2, at 9.

[67] Brief of Amicus Curiae, *supra* note 2, at 9.

[68] *See* United States v. Graham, 824 F.3d 421, 435-38 (4th Cir. 2016); Jordan v. United States, 138 S. Ct. 2700 (2018); United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016), *cert. granted sub nom.* Carpenter v. United States, 138 S.Ct. 2206 (2018).

[69] Carpenter v. United States, 138 S.Ct. at 2216. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 442 (1976). "As consumers turn over ever-increasing information to third parties as part of engaging in daily life, there have been vigorous criticisms of the doctrine as out of touch with the modern era and calls to amend it—or even abolish it entirely." *Geofence Warrants and the Fourth Amendment*, *supra* note 9, at 2510 n.35. (citing United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring); United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (en banc); 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(b), at 935-55 (5th ed.); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 213-15 (2006). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009)).

a person's physical presence compiled every day [and] every moment." [70]

When it comes to Step One Google LH information, the common practice (perhaps influenced by *Carpenter*) has been to require a warrant in order for the authorities to access the data in question.[71] In reality, however, there is no cause associated with the overwhelming majority of cell phone data accessed in the process.[72] The invasion, however, is so minimal that the lack of cause has not created a significant problem for authorities seeking warrants.[73]

A Step One geofence warrant seeks location information about individuals (or their devices) at a certain geographic area in a

---

[70] *Carpenter*, 138 S. Ct. at 2220; *see also Jones*, 565 U.S. at 415 (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"). *See* McLeod, *supra* note 4, at 549 ("it seems definitive that long-term monitoring of location data would implicate a reasonable expectation of privacy, triggering the conduct as a search and requiring a warrant").

[71] "In *Carpenter*, the Supreme Court extended the warrant requirement to 'cell-site location information' or 'CSLI' maintained by cellular service providers, reasoning that the privacy interest in one's movements, as discoverable through the CSLI, was an interest that modern society was prepared to recognize as reasonable." *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 734-35 (N.D. Will. 2020).

[72] That is not to say that there is no probable cause. Probable cause requires only "(i) a 'fair probability' that a crime has been committed and (ii) 'a fair probability that contraband or evidence of [that] crime will be found in a particular place.'" *In re* Search of Info. that is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 75 (2021) (citing Illinois v. Gates, 462 U.S. 213, 238 (1983)) (alteration in original). If the minimal invasion at issue were deemed to be a search, this cause should suffice to justify it.

[73] *See* United States v. James, 2019 WL 325231, at *3 (Jan. 25, 2019) (defendant argued that tower dump warrants were insufficiently particular because they "allowed law enforcement to identify the location of hundreds if not thousands of cell phone users on specific days during specific time frames.") The court, however, found the warrants sufficiently particular because they sought information that was "constrained—both geographically and temporally—to the robberies under investigation." *Id.*

limited timeframe.[74] The related search requires Google or any other private company to search through its databases and provide refined datasets. This is information that Google routinely receives and stores in *Sensorvault*, which assigns each device a unique identity and stores all LH data for use in marketing.[75] Google cannot find the requested location data without searching through the entirety of *Sensorvault*.[76]

The fact that the "companies look through their entire [location history] database" has led to comparisons between geofence warrants and general warrants.[77] In reality, however, and quite unlike general warrants, most people will never know that their data was reviewed in a Step One search, and the authorities will not learn anything about the identity of the owners of the phones.[78] It is no different from having one's fingerprints or DNA on file and available for comparison in new crime investigations.[79]

---

[74] That is different from what the Court dealt with in Carpenter: "[m]apping of a cell phone's location over the course of 127 days." *Carpenter*, at 2217. Moreover, "while *Riley* and *Carpenter* expressed concern over the ability of cell phones to track and recreate an individual's entire life stored on the cell phone, . . . the privacy interests at stake in those cases were violated because warrants were not obtained from neutral and detached judicial officers upon probable cause showings." *In re* Search Warrant Application for Geofence Location Data Stored at Google concerning Arson Investigation, 497 F. Supp. 3d 345, 364 (N.D. Ill. 2021) (citing *Carpenter*, 138 S. Ct. at 2221; *Riley*, 573 U.S. at 379-80).

[75] *Google Data and Geofence Warrant Process*, *supra* note 1.

[76] "When law enforcement wants information associated with a particular location, rather than a particular user, it can request 'tower dumps' — "download[s] of information on all the devices that connected to a particular cell site during a particular interval." *Geofence Warrants and the Fourth Amendment*, *supra* note 9, at 2516 n.79 (citing *Carpenter*, 138 S. Ct. at 2220; *see also* United States v. Adkinson, 916 F.3d 605, 608 (7th Cir. 2019)) (alteration in original) ("The difference between a tower dump and [S]tep [O]ne of Google's framework is obvious: the tower dump involves *only* data tied to the cell tower's location, while Google searches *all* of its location data even though *none* of it may be within the parameters of a geofence warrant.).

[77] *Id.* at 2516-18 ("A general warrant is one that "'specifie[s] only an offense," leaving "to the discretion of executing officials the decision as to which persons should be arrested and which places should be searched." (citing Steagald v. United States, 451 U.S. 204, 220 (1981))).

[78] In unusual cases, some private information may be revealed to the government officials who obtained the warrant, but it is a far cry from the overt and openly hostile searches to which this process is being compared.

[79] See Rychlak, *DNA Fingerprinting*, *supra* note 30.

To that end, and unlike the process in *Carpenter*, the third-party doctrine should apply to Step One data collection.[80] The third-party doctrine is based on the premise that a person's voluntary sharing of information with a third party overcomes any legitimate expectation of privacy in the information.[81] The *Carpenter* Court explained, "there is a world of difference between the limited types of personal information addressed in [earlier third-party doctrine cases] and the exhaustive chronicle of location information" collected today by third parties of all kinds.[82] Additionally, 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.[83] Google LH data, in contrast, is similar to the traditional third-party doctrine cases, and the LH data is actually shared with Google.

D. The Stored Communications Act

Although the Fourth Amendment's privacy rules may not trigger warrant requirements, the Stored Communications Act ("SCA") comes pretty close.[84] "The [SCA] governs how service providers such as Google handle the contents and records of their

---

[80] *Carpenter* rejected the argument that the third-party doctrine should extend to CSLI. 138 S. Ct. at 2219-20.

[81] See Smith v. Maryland, 442 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976). "Google has taken the position that the third-party doctrine should not defeat a cell-phone user's reasonable expectation of privacy in their location-history information because the user's sharing that information with a third-party such as Google is not truly voluntary." *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 737 n.4 (citing *Brief of Amicus Curiae*, *supra* note 2, at 20-22).

[82] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018); *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).

[83] *Carpenter*, 138 S. Ct. at 2220.

[84] *See* 18 U.S.C. §§ 2701 et seq.

users' stored electronic communications . . . .[85] In general, the SCA prohibits unauthorized access to stored communications, restricts the service provider's ability to disclose them to the government, and delineates the procedures law enforcement must follow . . . to compel production."[86]

Since a geofence request seeks the "contents" of Google users' electronic communications, authorities must obtain a warrant or its functional equivalent.[87] "The SCA . . . provides that the government may require a provider of electronic communication or remote computing services to disclose a subscriber's records . . . by obtaining either [] a warrant, or [] a court order [based] upon a showing of 'specific and articulable facts showing . . . reasonable

[85] "Google is the only tech company publicly known to release this kind of information to law enforcement specifically in response to geofence warrants. It is not clear how many other companies do the same." Leila Barghouty, *What are Geofence Warrants?*, THE MARKUP (Sept. 1, 2000, 8:00 AM), https://themarkup.org/the-breakdown/2020/09/01/geofence-police-warrants-smartphone-location-data. "Google is the most common recipient and the only one known to respond." *Geofence Warrants and the Fourth Amendment*, *supra* note 9.

[86] "The SCA draws a distinction between government access to the contents of electronic communications in 'electronic storage in an electronic communications system for one hundred and eighty days or less'—for which a warrant is invariably required—and access to the contents of electronic communications in "electronic storage in an electronic communications system for more than one hundred and eighty days' or contents of electronic communications 'in a remote computing service,' for which a warrant is required unless the government complies with certain notice procedures." Brief of Amicus Curiae, *supra* note 2, at 15 (quoting 18 U.S.C. § 2703(a), (b)).

[87] *Id.* at 11. *See* 18 U.S.C. § 2703(a), (b) (incorporating requirements of Fed. R. Crim. P. 41).

grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation.'"[88]

Thus, regardless of the Fourth Amendment or the third-party doctrine, the government is statutorily required to obtain a warrant or its functional equivalent and to satisfy all the substantive and procedural obligations attending the issuance of such documents. The question, however, remains as to whether a typical fact scenario provides sufficient probable cause to justify the warrant. It seems clear that privacy interests would be better served by requiring the warrant at Step Three and permitting the Step One information to be provided based on the third-party doctrine.

III. ANALYSIS

Geofence data is an effective and valuable crime-prevention tool. Provided that the authorities comply with the SCA, based on reason to believe that an unidentified suspect was in a specified geographic location during a limited time period, Step One Google LH information should be accessible even without a search warrant.

On the other hand, at Step Three, at which time the Google LH information data is de-anonymized, there is evidence that can and should be considered by a judge. At this point, specific phones have been identified, and the routes they have traversed may have been expanded and explored. The owners of these phones are the

---

[88] United States v. Ellis, 270 F. Supp.3d 1134, 1146-47 (N.D. Cal. 2017) (citing 18 U.S.C. §§ 2703(c)(1) and (d)). "The 'specific and articulable facts' standard under the SCA requires a higher showing than the certification required by the pen register statute, but does not require probable cause." "The provisions for authorizing a pen register and/or a trap and trace device under Title III of the Electronic Communications Privacy Act of 1986 ("ECPA"), codified as amended at 18 U.S.C. §§ 3121–3127 (referred to throughout as the "pen register statute"), require a government attorney merely to "certify" the relevance of the information likely to be obtained, without requiring a factual basis for the certification. 18 U.S.C. §§ 3122 and 3123 (requiring the court to enter "an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation")." *Id.* at 1146; *see also* Pretrial Order No. 3 Denying Motions to Suppress at 13-14, United States v. Ellis et al., No. 4:13-cr-00818-PJH, (No.337), https://www.govinfo.gov/content/pkg/USCOURTS-cand-4_13-cr-00818/pdf/USCOURTS-cand-4_13-cr-00818-9.pdf [https://perma.cc/57B2-8D6F].

people most likely to actually encounter a true search. It is at this point that evidence should be presented to a magistrate and a warrant obtained.

A. Probable Cause

In the Matter of the Search of Information that is Stored at the Premises Controlled by Google LLC, [89] the magistrate judge issued a memorandum opinion explaining his basis for issuing a geofence warrant at Step One.[90] He found that there was a fair probability that the search of Google's servers would uncover useful evidence pertaining to the identities of the suspects.

> First, there is more than a "fair probability" that the suspects were within the geofence during the time windows the government established. The requested geofence encompasses the [Redacted] center and its parking lot. The CCTV footage obtained by the government shows the suspects inside the [Redacted] center.
>
> Second, the government has evidence that the suspects were actually using cell phones during the time windows set in the warrant. The CCTV footage apparently shows the suspects utilizing their devices while inside the [Redacted] center.
>
> Third, the affidavit's failure to specifically allege that the suspects, while on their phones, were using applications or other features that would communicate location data to Google, is also not fatal to the warrant application. The probability that the phones were communicating location information to Google is, at the very least, "fair," and that is all that is required.

---

[89] *In re* Search of Info. that Is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62 (D.D.C. 2021).

[90] *Id.* at 75 (citing Illinois v. Gates, 462 U.S. 213, 238 (1983)). "[T]he core inquiry is whether the warrant application provides 'a substantial basis for concluding that a search would uncover evidence of wrongdoing' by 'demonstrat[ing] cause to believe that evidence is likely to be found at the place to be searched' and 'a nexus . . . between the item to be seized and criminal behavior.'" *Id.* (citing United States v. Griffith, 867 F.3d 1265, 1271 (D.C. Cir. 2017)). *See also* McLeod, *supra* note 4, at 553.

> Fourth, there is also a "fair probability" that Google is in possession of identifying information for the users of phones found within the geofence.[91]

Accordingly, the magistrate judge determined that probable cause existed for the issuance of the warrant.[92]

The warrant in that case came at Step One, but the analysis applies at Step Three (de-anonymizing) just as well. In fact, by that stage, there would be solid reasons to believe that everyone involved in any subsequent search would have been within the geofence area with their phone on their person and that Google would be able to provide the relevant information.[93] These people would be the most logical witnesses or suspects.[94]

B. The Minimal Invasion of Privacy

The Supreme Court has held that "it is untenable to conclude that property may not be searched unless its occupant is reasonably suspected of crime."[95] A search warrant "*may be issued when it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises*."[96]

When it comes to the geofence warrant process, the invasion or "search" at Step One is so minimal that most innocent people are not disturbed in any way and never even learn about it. The court in *In re Search of Information that Is Stored at the Premises Controlled by Google LLC* stated: *"[T]he geofence only provides cell phone users' whereabouts in a single area for a handful of minutes on the days in question, not the sum-total of their daily movements. Thus,*

---

[91] *In re Search of Info. that Is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 77-79.

[92] *Id.* at 79 ("[T]here is probable cause that the search will produce evidence useful to the government's investigation of criminal activity in question.").

[93] This renders moot the concern in *Riley v. California* and *Carpenter v. United States*, the ubiquity of cell phones and their common usage. *See Carpenter*, 138 S. Ct. at 2211; *Riley*, 573 U.S. at 395.

[94] "[T]he Fourth Amendment does not deal in precision, but rather in probability. That is, the government must demonstrate a fair probability that evidence of a crime will be located at a particular place, and a search warrant need not be rooted in pinpoint accuracy." *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning Arson Investigation, 497 F. Supp. 3d 345, 353 (N.D. Ill. 2020).

[95] Zurcher v. Stanford Daily, 436 U.S. 547, 559 (1978).

[96] *Id.*

viewed in proper context, the government's request is limited and reasonable."[97]

Even at Step Three, privacy invasions may be quite limited, but it is true: some people will likely be investigated for no reason other than that their phone was determined to have been at the scene of a crime or other incident.

The Supreme Court has recognized the "*ancient proposition of law*" that the public "has a right to every man's evidence."[98] When it comes to geofence data, Google (or the relevant service provider) is essentially a witness to a crime or other event and has relevant information in a database used to provide services to its users and advertisers. The public has a right to such evidence, and the Fourth Amendment does not bar the authorities from obtaining that evidence.

> The proper line of inquiry is not whether a search of location data could impact even one uninvolved person's privacy interest, but rather the reasonableness of the search, the probability of finding evidence at the location, and the particularity of the search request. Furthermore, it is also vital to repeat that the so-called "uninvolved individual" may actually be a witness to the crime. For example, the delivery truck driver, if present, could be a witness to the arson or suspicious vehicles driving to and from the arson site. The government is entitled to search for evidence of the crime pursuant to a valid warrant and that evidence includes the identity of witnesses to the offense.[99]

---

[97] *In re Search of Info. that Is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 81.

[98] United States v. Nixon, 418 U.S. 683, 709 (1974).

[99] In re Search Warrant Application for Geofence Location Data Stored at Google Concerning Arson Investigation, 497 F. Supp. 3d at 362. *See also* Carpenter v. United States, 138 S. Ct. 2206, 2247 (2018) (Alito, J., dissenting) ("The Court ignores the basic distinction between an actual search (dispatching law enforcement officers to enter private premises and root through private papers and effects) and an order merely requiring a party to look through its own records and produce specified documents. The former, which intrudes on personal privacy far more deeply, requires probable cause; the latter does not. Treating an order to produce like an actual search, as today's decision does, is revolutionary. It violates both the original understanding of the Fourth Amendment and more than a century of Supreme Court precedent.")

The mere fact than an uninvolved individual's privacy rights are impacted by a search, particularly one supported by a warrant, is not at all unusual.[100]

While executing warrants, governmental officers come across evidence [relating to] innocent people . . . all the time.[101] Recall the search of a home:

> The government might search a house for evidence and search the bedrooms of people not involved in the crime. That's not ideal, either for those people or for the government. Everyone would prefer a world in which the government always finds the bad guy and never learns anything about anyone other than the bad guy. But traditionally that has not been a Fourth Amendment requirement.[102]

In addressing this argument in the context of whether a requested warrant was overbroad, the court in *In re Search of Information that Is Stored at the Premises Controlled by Google LLC* stated:

> The geofence may also capture the location information for persons who are not suspects, namely the other customers inside the [Redacted] center.... For several reasons, the warrant's potential to collect location information from

---

[100] "For example, when a court authorizes the search of a house, the entire house is subject to the search, and this includes the most private areas of a house, such as bedrooms and bathrooms, of individuals who may not be involved in the crime but who nonetheless live in the premises, such as spouses and children." *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d at 361 (citing United States v. Reichling, 781 F.3d 883, 888 (7th Cir. 2015)). *See In re* Search Warrant Application for the Search of a Townhome Unit, No. 20 M 106, 2020 WL 1914769, at *1 (N.D. Ill. Apr. 20, 2020) (describing search protocol in electronic evidence searches). "In another context, a search of a person's cell phone reveals calendar entries of meetings, events, and text messages with uninvolved individuals, along with pictures that identify that uninvolved individual's location." *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d at 361.

[101] *See* Brinegar v. United States, 338 U.S. 160, 176 (1949) ("Because many situations which confront officers in the course of executing their duties are more or less ambiguous, room must be allowed for some mistakes on their part. But the mistakes must be those of reasonable [people], acting on facts leading sensibly to their conclusions of probability.").

[102] Kerr, *supra* note 56.

> these other individuals does not render it deficient.... As an initial matter, constitutionally permissible searches may infringe on the privacy interests of third persons—that is, persons who are not suspected of engaging in criminal activity. The Supreme Court has long recognized and accepted that third party privacy interests could be impacted by lawful searches.... The Fourth Amendment was not enacted to squelch reasonable investigative techniques because of the likelihood—or even certainty—that the privacy interests of third parties uninvolved in criminal activity would be implicated.... Rather, the Fourth Amendment seeks to ensure that privacy interests are not infringed by law enforcement activities without a showing of probable cause and a particularized description of the place to be searched and the things to be seized.[103]

Ybarra v. Illinois is often cited for the proposition that probable cause must be particularized for all persons that are subject to a search.[104] In that case, police obtained a warrant to search a tavern and the bartender for narcotics, but when they executed the search, bar patrons were there and they were also searched.[105] With a Step Three geofence warrant, however, officers would have no reason to go beyond the scope of the judicially-approved search. The government would have established to a judge's satisfaction that authorized location data would help identify perpetrators, co-conspirators, and witnesses within the

---

[103] Matter of Search of Info. that is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d at 82-84.

[104] Ybarra v. Illinois, 444 U.S. 85, 91 (1979). *See* Tim Cushing, *Virginia Court Blocks Geofence Warrant as Unconstitutionally Vague*, techdirt (Mar 9, 2022, 10:50 AM), https://www.techdirt.com/2022/03/09/virginia-court-blocks-geofence-warrant-as-unconstitutionally-vague/ ("Imagine if, in *Ybarra*, police knew someone in the bar possessed heroin, but they needed to identify who. Could a court authorize a warrant for police to search everyone in the bar to figure out who was the possessor? No. No court would properly authorize such a warrant." (quoting Letter from David Oblon, Judge, Fairfax Cnty. Cir. Ct., to Scott Reever, Detective, Fairfax Cnyt. Police Dep't (Feb. 24, 2022), https://www.fairfaxcounty.gov/circuit/sites/circuit/files/assets/documents/pdf/opinions/km-2022-79-in-matter-search-info-premises-google-020822.pdf [https://perma.cc/Q2JQ-XRBL])).

[105] *Ybarra*, 444 U.S. at 92-93.

identified area. Such a process is "*sufficiently particular to avoid any concerns resulting from* Ybarra."[106]

Moreover, capturing and reviewing Google LH data over a limited time in a specified perimeter provides only limited information about the owner. That is a far cry from the search of a person in a tavern. There is no physical intrusion upon a person's body involved in geofence searches; "it is more akin to a search for specific information within a place for which the government has obtained a search warrant."[107]

CONCLUSION

Geofence warrants, like all warrants, are subject to judicial oversight, which ensures they are not used indiscriminately or without probable cause. Provided they are narrowly tailored to a specific geographic area and time frame, and used only when there is probable cause to believe the data will be relevant to a criminal investigation, they are effective tools for law enforcement. That is particularly true in cases where traditional investigative methods have been exhausted.

A Fourth Amendment warrant should not be required at Step One, when all phones within the geofence are identified through a process that involves the provider searching across all of its data. At this phase, the invasion of privacy is minimal, and the third-party doctrine should come into play. The Stored Communications Act should be amended to make clear that a warrant or court order is not needed until Step Three, the point of de-anonymization. That

---

[106] *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning Arson Investigation, 497 F. Supp. 3d 345, 362 n.6 (N.D. Ill. 2020). *See also In re* Warrant Application for Use of Canvassing Cell-Site Simulator 654 F. Supp. 3d 694 (N.D. Ill. 2023) (citing United States v. Chatrie, 590 F. Supp. 3d 901, 928-34 (E.D. Va. 2022) (discussing the preferred test for a geofence warrant that the government must establish probable cause)).

[107] *In re* Warrant Application for Use of Canvassing Cell-Site Simulator, 654 F. Supp. 3d. 694 (N.D. Ill. 2023). *See* Kerr, *supra* note 56 ("I don't see how *Ybarra* can be relevant to the Fourth Amendment standard for geofence warrants.").

is where citizens might actually be searched. That is where judicial supervision would do the best.[108]

[108] The Supreme Court has already upheld the use of similar investigative techniques, such as pen registers, trap and trace devices, and "honeypot" false webpages. "A honeypot website is meant to capture users that are attracted to the illicit content that site may provide." Martin Novak, *Digital Evidence in Appeals of Criminal Cases Before the U.S. Courts of Appeal: A Review of Decisions and Examination of the Legal Landscape from 2016 – 2020*, 17(3) J. OF DIGIT. FORENSICS, SEC. & L. 1, n. 50 (2022), https://commons.erau.edu/cgi/viewcontent.cgi?article=1734&context=jdfsl [https://perma.cc/U32Q-3GVK] (last visited Feb. 23, 2024).