William & Mary Bill of Rights Journal

Volume *30 (2021-2022)*
Issue 2 *Algorithms and the Bill of Rights*

Article 13

12-2021

Geofence Warrants: Geolocating the Fourth Amendment

A. Reed McLeod

GEOFENCE WARRANTS: GEOLOCATING THE FOURTH AMENDMENT

A. Reed McLeod*

INTRODUCTION

Modern phones carry a unique and diverse array of sensors, used primarily to provide the user with what we now expect of any given smartphone. For example, accelerometers measure acceleration in three-dimensional space, and in combination with your phone's gyroscope, enable it to detect when you want your applications in portrait or landscape mode.[1] When these two sensors, and others as well, are correlated with inputs from GPS satellites, an increasingly detailed picture of a user's location is formed.[2] This location data provides an amazing array of map

* JD Candidate, William & Mary Law School, Class of 2022. A heartfelt thanks to my friends and family. Without their support, I could not have completed this Note, nor any part of my academic career.

[1] David Nield, *All the Sensors in Your Smartphone, and How They Work*, GIZMODO (June 29, 2020, 10:38 AM), https://gizmodo.com/all-the-sensors-in-your-smartphone-and-how-they-work-1797121002.

[2] *See id.*

services and has, to some extent, trained consumers to depend on these services for travel to unfamiliar destinations.[3]

Such services come at a cost, minor to most: providing user location data to a company for its own use. Often, this has no individual consequence. Most companies use the location data to turn a profit. For example, Google uses such data to better individualize and target advertisement.[4] Increasingly, however, this location data is being requested by the government in the form a "geofence" warrant. When a geofence warrant is served on Google, this warrant queries *every* user in Google's database of location data, called the SensorVault.[5] Very few known investigative tools have the scope, in both space and time, to affect every Google user who has, at one time or another, enabled Location History on their Android device or Google account.[6]

This Note begins by focusing on the technology and procedure of geofence warrants in Part I. Because an understanding of both the technology and procedure is ultimately required to make any headway in later legal analysis, this step is necessary. The heart of the legal analysis is undertaken in Parts II and III.

In Part II, this Note argues that law enforcement requests for location data require a warrant: either because of the expectation of privacy in location data proposed by cases such as *Carpenter v. United States*[7] or because some courts have found that *Carpenter*'s holding must mean location data should be treated as content, which triggers a statutory warrant requirement under the Stored Communications Act.[8]

In Part III, having established a warrant is necessary, this Note further argues geofence warrants can satisfy the probable cause and particularity requirements of the Fourth Amendment. For probable cause, the government must narrowly tailor the warrant to objective, established facts, avoiding the incidental capture of other users as much as possible. For particularity, in a similar sense, the government must use *ex ante* limitations on the warrant that restrict the capture of data to only those individual users for whom probable cause has been established, permitting as little officer discretion in the execution of the warrant as possible. Courts view the Fourth

---

[3] *See* Nathaniel Sobel, *Do Geofence Warrants Violate the Fourth Amendment?*, LAWFARE (Feb. 24, 2020, 1:03 PM), https://www.lawfareblog.com/do-geofence-warrants-violate-fourth-amendment [https://perma.cc/3AHB-6B3T].

[4] *Privacy & Terms: How Google Uses Location Information*, GOOGLE, https://policies.google.com/technologies/location-data?hl=en-US [https://perma.cc/7NVK-LK6M] (last visited Dec. 13, 2021).

[5] 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/WSG3-ZFNA].

[6] *See* Jennifer Lynch, *Google's Sensorvault Can Tell Police Where You've Been*, ELEC. FRONTIER FOUND. (Apr. 18, 2019), https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been [https://perma.cc/9TR2-2PBF].

[7] 138 S. Ct. 2206 (2018).

[8] 18 U.S.C. §§ 2701–2713.

Amendment through the lens of what is reasonable: a narrow geofence warrant is better, all things considered. To effectively tackle these complex Fourth Amendment issues, this Note begins with technology and procedure of a geofence warrant itself.

I. THE TECHNOLOGY AND PROCEDURE OF GEOFENCE WARRANTS

On a Monday afternoon in May 2019, surveillance footage captured images of a man holding a cell phone up to his ear outside the Call Federal Credit Union in Midlothian, Virginia.[9] Moments later, police alleged that same individual entered the bank and robbed it of $195,000 in cash, fleeing the scene with the money.[10] After weeks passed with no leads, law enforcement applied for a search warrant.[11] In the probable cause affidavit, law enforcement proposed that, as a result of the observed cell phone use outside the credit union, and because many cell phones use the Android operating system, evidence of the bank robbery might well be on Google's servers.[12] The evidence specifically sought was the unknown suspect's location data, which could show his movements directly before, during, and after the robbery.[13]

The search warrant briefly described above is the topic of this Note and is known as a "geofence" warrant. Their structure is usually common: a suspect is observed with a cell phone or assumed to have one on his or her person because of their ubiquity in daily life.[14] Two premises are assumed from there. First, many phones either run Android's operating system or interface with a Google Account and Google's servers when accessed by a non-Android phone.[15] Second, many users enable Google location services when setting up a Google Account.[16] With those premises in hand,

---

[9] Deanna Paul, *Alleged Bank Robber Accuses Police of Illegally Using Google Location Data to Catch Him*, WASH. POST (Nov. 22, 2019), https://www.washingtonpost.com/technology/2019/11/21/bank-robber-accuses-police-illegally-using-google-location-data-catch-him/ [https://perma.cc/QA85-VZ6W].

[10] *Id.*

[11] *See* Affidavit for Search Warrant at 1, United States v. Chatrie, No. 3:19-cr-130 (E.D. Va. Sept. 17, 2019), https://www.nacdl.org/getattachment/fc0182fd-fe6c-452f-b31f-d7a63acc135a/edva-geofence-warrant.pdf [https://perma.cc/ZMU4-8QGD].

[12] *Id.* at Attachment III, 4–5.

[13] *Id.* at Attachment II, 2–3.

[14] *See, e.g.*, Application for Search Warrant at Attachment III, In the Matter of Accounts associated devices that were inside the following geographical area: NW Corner 35.7840570°, -78.644821°, NE Corner 35.784018°, -78.643561°, SE Corner 35.782758°, -78.643574°, SW Corner 35.782797°, -78.644853° during the following time frame: 1930 hours Eastern and 2200 hours Eastern, on 3/16/2017, data maintained on computer servers controlled by Google, Inc. (N.C. Dist. Ct. for Dist. of Wake Cnty. May 5, 2017) [hereinafter Raleigh Devices Geofence Warrant], https://www.documentcloud.org/documents/4388574-20170505-arson-warrant.html#document/p3/a410682 [https://perma.cc/B5JC-DH5V] (assuming that an unknown suspect has a cell phone without any corroborating evidence to indicate that fact).

[15] *See id.*

[16] *See id.*

Google's SensorVault—the database that holds the location data of all Google users—may very well hold evidence of the specific crime at hand. This final fact explains much, because the SensorVault likely holds billions of records of relatively mundane activity, among which could well be evidence of any given crime.

A perhaps more descriptive name for a geofence warrant is a reverse location history search warrant.[17] This is because the search focuses on a given location (and time) to find an unknown suspect or witness to a crime.[18] The bank robbery case is illustrative. In that case, law enforcement's warrant application proposed that Google conduct a SensorVault search query where the geographic boundaries of the search would be limited to a 150-meter circle centered on the Credit Union.[19] The query would be further limited by time: the hour-long span during which the robbery occurred.[20] Google's production returns would include anonymized location data of any user within the boundaries.[21] Individuals included in these production returns are subject to discovery only because of geographic and time constraints. As such, innocent individuals with no direct relation to the crime can be and often are included in the anonymized device IDs.[22]

Commonly, and sometimes referred to as "step one" of the procedure, the device IDs returned to law enforcement are subject to analysis: executing officers will sift through the anonymized data for patterns that suggest which of the anonymized accounts are persons of interest to the crime and which ones are not.[23] In the bank robbery example, nineteen device IDs were returned within the given boundaries.[24] Surveillance footage showed that there was only one visible suspect during the robbery.[25] Unclear as to which device ID was the suspect's phone, law enforcement refined their interest in the location data to nine of the nineteen device IDs.[26]

Beyond this point, some geofence warrants rely on the initial authority of the warrant for more data in a second round, refined by the data of step one. This can

---

[17] Paul, *supra* note 9.

[18] Raleigh Devices Geofence Warrant, *supra* note 14, at Attachment II (establishing two metrics—(1) geographic space and (2) recorded time—to restrict the SensorVault search query).

[19] *See* Affidavit for Search Warrant, *supra* note 11, Attachment II at 3.

[20] *Id.* at 2.

[21] *Id.*

[22] *See* Brief Amicus Curiae of Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant at 12–14, United States v. Chatrie, No. 3:19-cr-130 (E.D. Va. Dec. 23, 2019) [hereinafter Google Amicus Brief].

[23] *See* Valentino-DeVries, *supra* note 5.

[24] Frank Green, *Defense Challenges Use of Google Location Data from Everyone in Vicinity of Hull Street Road Bank Robbery*, RICHMOND TIMES-DISPATCH (Jan. 23, 2020), https://richmond.com/news/local/crime/defense-challenges-use-of-google-location-data-from-everyone-in-vicinity-of-hull-street-road/article_9e4f9ca6-d092-5f07-b932-b111553a114d.html [https://perma.cc/DU4H-PUL6].

[25] *See* Sobel, *supra* note 3.

[26] *See* Green, *supra* note 24.

be referred to as "step two" of the procedure: law enforcement obtains further information on these refined device IDs beyond the initial space and time constraints.[27] As the company usually subjected to such legal procedures, Google explained that "law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request."[28] While this is usually limited by a time constraint listed in the original warrant,[29] it is not usually limited by any space or geographic constraint. As a result, the refined device ID's location data in this step can be traced as far as it may have traveled based on this original time constraint.[30]

Using the anonymized data from step one, and step two if so conducted, law enforcement officers interpret and analyze the returns to try to determine which is from a suspect, witness, or unhelpful bystander. This can be referred to as "step three." Following this, law enforcement often attempts to obtain further legal process to de-anonymize the returns. In some examples, law enforcement relies on the original search warrant to "compel Google to provide account-identifying information for the anonymized device numbers that [law enforcement] determines are relevant to the investigation."[31] In most cases, Google will provide accompanying information related to the Google account more generally, called subscriber information, which can include a name and a linked Gmail account.[32] Returning to the bank robbery as an example, law enforcement compelled Google to provide non-anonymized information on three persons.[33]

Armed with basic information on these suspects, and correlating this data with eyewitness evidence,[34] law enforcement arrived at the home of Okello Chatrie, the alleged perpetrator. Prosecutors obtained an indictment against Chatrie for the bank robbery.[35] In *United States v. Chatrie*, now before the U.S. District Court of the

---

[27] Google Amicus Brief, *supra* note 22, at 13–14.

[28] *Id.*

[29] *See* Affidavit of Scott Kibbey, In the Matter of the Search of Information Regarding Accounts Associated with Certain Location and Date Information, Maintained on Computer Servers Controlled by Google, Inc. at 9, United States v. Guevara-Gonzales, No. 1:18-mj-00169-ML (W.D. Tex. Mar. 14, 2018), ECF No. 9-1; *see also* Raleigh Devices Geofence Warrant, *supra* note 14, Attachment I ¶ 3 (describing that after an initial review of anonymized device IDs, "Google, Inc. shall produce 'contextual data points with points of travel outside of the geographic area'" for a further thirty minutes before and after the original search parameters).

[30] *See* Valentino-DeVries, *supra* note 5 (visualizing the scope of the location information provided at this stage of the process).

[31] *See* Google Amicus Brief, *supra* note 22, at 14.

[32] *See id.*

[33] Sobel, *supra* note 3.

[34] *See id.*

[35] U.S. Attorney's Office, E.D. Va., Press Release, *Man Indicted for Armed Robbery of Credit Union*, U.S. Dep't of Just. (Sept. 18, 2019), https://www.justice.gov/usao-edva/pr/man-indicted-armed-robbery-credit-union [https://perma.cc/6CZR-W3Q5].

Eastern District of Virginia, the defendant has filed a motion to suppress the evidence obtained through the geofence warrant, claiming the warrant is an "unlawful and unconstitutional general warrant . . . both overbroad and lack[ing] the particularity required by the Fourth Amendment."[36] The case remains in preliminary litigation and a ruling on whether to suppress the evidence is outstanding.[37]

It will be useful to summarize the procedure for clarity's sake. A geofence warrant typically proceeds as follows: After a crime occurs at location *x*, using Google maps, law enforcement overlays a circle centered on a coordinate at location *x* or uses a set of coordinates to form a simple polygon that encompasses location *x*.[38] In addition, they choose a time frame within which the suspect or suspects were likely to be present at location *x*.[39] Using these geographic and temporal parameters, or multiples of them, law enforcement applies for a warrant that would compel Google to run a search query for all possible Google users that could have been present within the parameters.[40] The anonymized device IDs given by Google show the location data of users who were in the constraints. In some instances, the police will use this data to refine their search, either seeking further legal process or relying on the authority of the initial warrant. Sometimes, when relying on the initial warrant, law enforcement will compel information about these users in increasing levels of detail *beyond* the initial constraints, relying on other constraints in the initial warrant.[41] Finally, in some cases, the police will compel the subscriber information of those device IDs narrowed down throughout this process.

It seems unmistakable that this investigative tool holds great potential for solving complex crimes that would otherwise never be solved. For this, and other reasons, the use of these geofence warrants is becoming more and more common.[42] Google estimates that the company has seen a "1,500% increase in the number of geofence requests [] received in 2018 compared to 2017; and to date, the rate has increased over 500% from 2018 to 2019."[43]

Examples of geofence warrants like the one described above emphasize that trial courts will face unique and novel questions that implicate our complicated relationship with technology, monopolized markets, and the ubiquity of smartphone use. To address this, this Part continues in two short subparts. First, although user privacy has become

---

[36] Defendant Okello Chatrie's Motion to Suppress Evidence Obtained from a "Geofence" General Warrant at 1, United States v. Chatrie, No. 3:19-cr-00130-MHL (E.D. Va. Oct. 29, 2019), ECF No. 29.

[37] United States v. Chatrie (3:19-cr-00130), COURTLISTENER, https://www.courtlistener.com/docket/16215471/united-states-v-chatrie/ [https://perma.cc/27BT-RA62] (last visited Dec. 13, 2021).

[38] *See* Lynch, *supra* note 6.

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] Google Amicus Brief, *supra* note 22, at 2.

[43] *Id.* at 3.

a hot button issue, location data is so valuable that data companies have an incentive to encourage users to provide very precise movement patterns. This profit motive outweighs privacy concerns and ensures that geofence warrants will be an issue for the immediate future. Second, the average user (and legal practitioner) is likely unaware of the accuracy of modern location tracking. This accuracy influences the analysis of whether society is prepared to recognize an expectation of privacy in location data and whether location data can be construed as substantive content in and of itself.

A. The Value of Location Data

Here, two main points are stressed. First, the location data retained in Google's SensorVault implicates a vast number of Americans: potentially anyone with a Google account that enabled Location History at one time in the past.[44] Second, because of the profit model of advertising, this location data is more valuable than most realize. These two premises emphasize many other aspects of the issues described throughout, namely that this investigative tool is powerful, can affect millions of Americans, and is likely to remain relevant for some time.

Google began its rise to data supremacy in the online search business. While not without competitors in online searches, Google is currently peerless in terms of market share and profit.[45] It is projected that Google will have earned $39.58 billion through U.S. advertising in 2020 alone.[46] Such profits are driven by innovation, particularly by algorithmically tailoring advertising to consumers' preferences, which can and does use location data provided by user accounts which have enabled Google's Location History feature.[47]

The specific way that Google tracks location is described further below.[48] Setting aside the precise technological means, to enable the full functionality of an Android phone, or if using certain apps on an iOS phone, a user must set up a Google account. Google then prompts the user to enable Location History services. For most Android users, this is one prompt among many, of which some percentage will enable such

---

[44] Although it is very likely law enforcement requests geolocation information from other data companies, this discussion focuses on Google because their collection and retention of geolocation data has produced the most public scrutiny and analysis.

[45] According to open-source statistics site Statista, as of June 2021, Google had a search engine market share of 87.76 percent. Joseph Johnson, *Global Market Share of Search Engines 2010–2020*, STATISTA (Oct. 14, 2020), https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/ [https://perma.cc/TX9D-JF9W].

[46] Lauren Feiner, *Google U.S. Ad Revenue Will Drop for the First Time This Year, eMarketer Says*, CNBC (June 22, 2020, 10:24 AM), https://www.cnbc.com/2020/06/22/google-ad-revenue-will-drop-this-year-emarketer-says.html [https://perma.cc/A3DP-95NC].

[47] Google has been in the location tracking business since at least 2009. *See* Ian Paul, *Google Latitude Service Lets You Track Your Friends: How It Works*, PCWORLD (Feb. 4, 2009, 7:42 AM), https://www.pcworld.com/article/158909/google_latitude_tracks.html [https://perma.cc/B4MM-PHJ3].

[48] *See infra* Section I.B.

services.[49] Just like searches, which are free, Google's Location History provides users with enhanced functionality for the free Google Maps application and others.[50] Just like searches,[51] Location History is attributable to a certain Google account, and optimizes the picture of that user overall.[52] Location data can sometimes be gleaned by other means, including applications on the Android OS which request it. These Location History users can provide better advertising revenue, which itself is a demonstrable means of enhancing profits.[53] The number of Android OS phone users utilizing Location History services is projected to reach 131 million in 2021.[54]

The overall point made here is that Google, and companies like it, have a strong incentive to promote the use of location services. This will affect a large portion of the American population. It is clear that enough people do opt in to some form of location data sharing to make Google's SensorVault dataset an invaluable tool for tackling serious problems,[55] including the pursuit of unknown suspects.

B. The Accuracy of Location Data

With a few simple affirmative responses, a user may transmit their location in return for increased functionality of their phone. Here, it is proposed that the accuracy in this data makes a difference in legal analysis. In short, the patterns revealed in location data represent something like a personal log of an individual's interactions with society.

A smartphone device[56] with a Google account, data services on, and Location History enabled will transmit the location of that device based on multiple different

---

[49] Precise statistics about the use of Google Location History are not publicly available.

[50] *See Privacy & Terms: How Google Uses Location Information*, GOOGLE, https://policies.google.com/technologies/location-data [https://perma.cc/H7GL-YSBU] (last visited Dec. 13, 2021).

[51] *See Privacy & Terms: Advertising*, GOOGLE, https://policies.google.com/technologies/ads?hl=en-US [https://perma.cc/4YLE-J6V9] (noting that advertising might be "based on your app activity or . . . web activity" connected to a Google account) (last visited Dec. 13, 2021).

[52] *See* GOOGLE, *supra* note 50 (noting that, if a user opts in and is reporting location in their device settings, "the precise location of your signed-in devices will be collected and stored, even when you're not actively using a Google product or service.").

[53] *See* Mike Brown, *How Google Maps Will Make Money on Your Restaurant Searches*, INVERSE (Apr. 28, 2017, 9:36 AM), https://www.inverse.com/article/30916-google-maps-makes-money [https://perma.cc/SV4R-ZNHG].

[54] S. O'Dea, *Android Smartphone Users in the United States 2014–2022*, STATISTA (Mar. 1, 2020), https://www.statista.com/statistics/232786/forecast-of-android-users-in-the-us/ [https://perma.cc/7MAT-Q8KU].

[55] Tony Romm et al., *U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus*, WASH. POST (Mar. 17, 2020, 9:15 PM), https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/ [https://perma.cc/8KT7-E6F7].

[56] This includes iOS phones that have installed a Google account and enabled Location History.

inputs: "GPS and Bluetooth signals, Wi-Fi connections, [] cellular networks"[57] all provide a reading on the phone, as well as internal sensors like "accelerometer[s] and barometer sensors, . . . gyrometer and magnetometer sensors . . . ."[58] 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."[59] Thus, a geofence warrant, which relies on this location data, can precisely follow a user from the scene of a crime to their home and every place in between: be that a doctor's clinic, middle school, or place of worship.[60]

Everyday users and legal practitioners alike may not realize the accuracy and scope of the location data obtained by Google. In its *Amicus* Brief, Google had to actively differentiate Location History data from other types of cell phone data when discussing it in the context of geofence warrants.[61] Thinking back to the bank robbery example, the *Chatrie* case, the parties there made comparisons between Google Location History data to recent precedent on cell phone location data.[62] But representatives for Google clarified Location History data as unique. This location data is predicated on opting in and is "considerably more precise than other kinds of location data" considered by the Supreme Court and other courts.[63]

The accuracy of this data, when combined with an option to opt into the service, has led representatives of Google to characterize the data as more akin to a journal, or personal log, of the individual's public movements.[64] This admission is meaningful because it recognizes and elevates the decision made by the user in accepting location services. Only after user action is there a log of personalized location data drawn from the sensors described above.[65] Further, and regardless of a user's volition,

---

[57] *See* Google Amicus Brief, *supra* note 22, at 7. Although Google emphasizes the many steps a user must make to configure a device to send precise data to the Google Sensorvault, location-reporting settings default to the highest accuracy possible.

[58] Letter from Susan Molinari, Vice President, Google, to Senators Richard Blumenthal & Edward Markey (Jan. 12, 2018), https://www.blumenthal.senate.gov/imo/media/doc/05.11.2018%20-%20FTC%20-%20Google%20Location%20History.pdf [https://perma.cc/HHK9-3VH6].

[59] Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (demonstrating the accuracy of the technology in the context of apps which use the same methods of location tracking).

[60] *Id.* (documenting that similar forms of location data tracking showed patterns of movement within a pregnancy clinic, children's schoolyard, and megachurch). Geofence warrants raise other important constitutional questions, chief among them First Amendment concerns. Those questions are beyond the scope of this Note, which focuses on the Fourth Amendment issues.

[61] Google Amicus Brief, *supra* note 22, at 8–10.

[62] Explained in greater detail *infra* at Part II.

[63] Google Amicus Brief, *supra* note 22, at 9–10.

[64] *Id.* at 6.

[65] *See* Letter from Senators Richard Blumenthal & Edward J. Markey to Joseph Simmons, FTC Chairperson (May 11, 2018), https://www.blumenthal.senate.gov/imo/media/doc/05.11.2018%20-%20FTC%20-%20Google%20Location%20History.pdf [https://perma.cc/HHK9

the accuracy of this data can unto itself be reflective of habits, patterns, and perhaps even personality characteristics.[66] This data is openly comparable to other forms of personal logging, such as diaries, itineraries, or schedules, suggesting a strong privacy interest for that data. Relying on these ideas, Part II examines whether a reasonable expectation of privacy should exist in location data.

II. LOCATION DATA: IS A WARRANT REQUIRED?

A. The Retrieval of Location Data Is a Fourth Amendment Event Requiring a Warrant

The text of the Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[67]

Historical analysis of this period strongly suggests that authors of the Fourth Amendment structured its language, at least in part, to respond to and prevent general warrants.[68] These types of warrants typically left a great deal of discretion to the officer who held the warrant, leading to the usual problems with a subjective application of authority, such as arbitrary and oppressive enforcement.[69] In response, the authors of the amendment included what is known as the warrant clause—the second part of the amendment—which includes the requirements of probable cause, the swearing by oath or affirmation to the facts supporting the warrant, and the particularity requirement.[70]

-3VH6] ("Once a user allows Location History in one application, they enter into the expansive and continuous collection of location data . . . .").

[66] Clemens Stachl et al., *Predicting Personality from Patterns of Behavior Collected with Smartphones*, 117 PROCEEDINGS OF THE NAT'L ACAD. OF SCI. 17680–17681, https://www.pnas.org/content/pnas/117/30/17680.full.pdf [https://perma.cc/9P63-C8XT].

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

[68] *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 625, 655–65 (1999); *see also* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 1044–51 (2011) (noting that proposals of a right against unreasonable searches and seizures by "Madison, Adams, and [] previous state constitutional provisions all condemned general warrants.").

[69] *See* Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J.L. & TECH. 120, 123 (2007).

[70] An analysis of two of these requirements—probable cause and particularity—is

As the Supreme Court has noted, it is "perfectly clear that the evil the Amendment was designed to prevent was broader than the abuse of a general warrant. Unreasonable searches or seizures conducted without any warrant at all are condemned by the plain language of the first clause of the Amendment."[71] As such, a legal request that does not qualify as a search or seizure does not require a warrant at all.

This Note attempts to answer the threshold question as to whether this legal request for Location History information is a search, seizure, or subject to a statutory requirement necessitating a warrant. The ultimate conclusion here is that recent precedent suggests a reasonable expectation of privacy in location data.

1. Reasonable Expectation of Privacy in Location Data

As stated, it is presumptively unreasonable to conduct a search or seizure of data without a warrant.[72] As such, and in practical terms, the Note is here inquiring whether, because the request for that data is *not* a search or seizure, the government could request location data from a company like Google with legal process short of a warrant, such as a subpoena.

It is a possible oversimplification, but in most early claims of violations of the Fourth Amendment, the defendant usually focused on some sort of physical trespass, which itself constituted a "search."[73] As a result, for most of the Court's history, the physicality of searches meant that the rights protected by the Fourth Amendment were usually defined as tangible property rights.[74] Recently, members of the Court championed this idea as still valid: a trespass against a traditionally protected area for the purpose of retrieving evidence is a search.[75]

Technology introduced new issues. Over time, the government could capture the intangible aspects of life in the telephone wires and receivers that carry our private conversations. These were initially not given Fourth Amendment protection.[76] An emphasis on tangible property rights remained the sole theoretical basis for the Fourth Amendment until the seminal case of *Katz v. United States*.[77] In that case, the

undertaken in Part III, after first answering the question of whether a warrant is initially required. *Infra* Part III.

[71] Payton v. New York, 445 U.S. 573, 585 (1980).

[72] *Id.*

[73] *See* Clancy, *supra* note 68, at 1058.

[74] *See* Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 562, 578–79 (1996).

[75] United States v. Jones, 565 U.S. 400, 404 (2012) (holding that the physical occupation of private property, a car, is a search within the meaning of the Fourth Amendment when it was adopted). *Jones* was concerned with a government GPS tracking device adhered to a car. *Id.* at 402. *Jones* is discussed below, at length, in Section II.A.2.

[76] Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

[77] Katz v. United States, 389 U.S. 347 (1967).

court expanded the definition of a search to include governmental intrusions that invaded a reasonable expectation of privacy.[78]

In *Katz*, the Court considered a government listening device placed outside a private telephone booth, a booth in which the government suspected Katz was conducting illegal gambling activity over the telephone.[79] Emphasizing that the Fourth Amendment protected the privacy interests of a citizen, the majority extended Fourth Amendment protection to the intangible privacy interest Katz held in his private conversation, stating that "the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures . . . ."[80] The majority opinion sketched out the idea of a right to privacy against unreasonable searches and seizures, but without a formal test for establishing when a person could invoke this right. It is Justice Harlan's concurrence in *Katz* that provides the test and establishes when a search has been conducted against intangible privacy interests. Because the other opinions lacked a clear standard, Harlan's formulation has proved influential since the decision. The test is as follows: A person has a reasonable expectation of privacy in their communications where that person subjectively expected such privacy and where society would recognize that expectation as an objectively reasonable one.[81]

This appears straightforward enough, but almost immediately, the *Katz* reasonable expectation of privacy test was subject to caveats which complicate the analysis. For geofence warrants, one exception is especially relevant: "what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[82]

Because location data is held as a record by another party, an analysis as to whether accessing location data in a search implicates a doctrine known as the third-party doctrine. The third-party doctrine was first sketched out in the context of cases involving simple business records in the late 1970s.[83] In sum, the Court has described the third-party doctrine as where a person assumes a "risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[84] The third-party doctrine "stems from a particular conception of privacy that views Fourth Amendment privacy as constituting a form of total secrecy."[85] This doctrine assumes that when the information is provided to a third party, the secrecy

---

[78] *See id.*

[79] *Id.* at 347, 349.

[80] *Id.* at 353.

[81] *Id.* at 361 (Harlan, J., concurring).

[82] *Id.* at 351.

[83] *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) (no reasonable expectation of privacy in financial records provided from a bank to the government); *see also* Smith v. Maryland, 442 U.S. 735, 743 (1979) (no reasonable expectation of privacy in dialed numbers provided from a phone company to the government).

[84] *Miller*, 425 U.S. at 443.

[85] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1136 (2002).

barrier is broken and no reasonable expectation of privacy can attach. This is an important point. If a court finds this doctrine present for the data subject to an intrusion, no warrant need be issued for the data.

Some scholars have argued that this doctrine is both rational and serves laudable goals.[86] Rather than waiving a reasonable expectation of privacy, it makes more sense to say that "[t]hird-party disclosure eliminates privacy because the target voluntary consents to [a] disclosure . . ." of ostensibly private information.[87] Further, the third-party doctrine serves important goals. It permits observation of those crimes that would completely take place by agents of the true criminal, be they co-conspirators or an unwitting business; and, it provides clarity to law enforcement in an unclear area of law, emphasizing which private data will definitely require a warrant.[88]

In response to these rational aims, however, consider a Google user's consent to Location History (or most forms of consent to high-tech data collection for that matter). Users either opt in with less than explicit notice given to them, or even with good notice, without a full realization of the potential consequences to their privacy if they opt in.[89] Second, users may understand the notice they have been given, but misunderstand the accuracy of the movement patterns as expressed in the location data collected by tech companies.[90] Where a user cannot properly understand the full ramifications of the initial acceptance of data collection, consent is a fiction that does not really represent true acceptance.[91] Justice Sotomayor generally agrees with this point, stating that the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[92]

Determining whether the third-party doctrine applies to location data is premature without first considering two cases on point: *Jones* and *Carpenter*. To some extent, both cases incorporate a discussion of the third-party doctrine and of reasonable expectations of privacy in location data. So, with the understanding developed above, this Note continues by discussing these cases to determine whether a search occurs in requesting location data.

---

[86] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588 (2009).

[87] *Id.*

[88] *Id.* at 575–76, 581–82.

[89] *See Every Step You Take: How Deceptive Design Lets Google Track Users 24/7*, NORWEGIAN CONSUMER COUNCIL (FORBRUKERRÅDET) 26–28, 36–37 (2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf [https://perma.cc/9E36-T7EG].

[90] *See supra* Section I.B.

[91] *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1885–88, 1894 (2013).

[92] *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

2. *Jones* and *Carpenter*: The Supreme Court Considers Location Data

As explained directly above, when determining whether government requests for location data invade a reasonable expectation of privacy, and thus constitute a Fourth Amendment search, the storage of location data with a third party will implicate the third-party doctrine. In terms of clarifying this analysis, the good news is that the Supreme Court has two recent cases, *Jones* and *Carpenter*, explaining the Court's thinking on location data and the third-party doctrine.[93] The bad news for these cases is that only *Jones'*s concurrences are truly elucidating to broader location data issues and *Carpenter* explicitly claims it is decided on narrow grounds.[94] Said another way, both cases are very applicable to questions regarding geofence warrants, but the breadth of their reach is very unclear. Still, this Note argues that both cases suggest a person has a reasonable expectation of privacy in their location data, and thus the Fourth Amendment presumes a warrant is required for location data.

In *Jones*, at issue was the government's use of a GPS device on a vehicle, placed in violation of the warrant that permitted its use by being installed in Maryland rather than in the District of Columbia.[95] The government tracked the defendant's vehicle for twenty-eight days via a GPS device placed on the vehicle by the police department, and the defendant attempted to suppress the evidence obtained from it.[96] In holding that the "installation of a GPS device . . . to monitor the vehicle's movements" was a search, the Court relied on the government's physical trespass of the car, rather than the *Katz* expectation of privacy test.[97] This reestablished the continued validity of a "search" being indicated by a physical trespass on private property.[98] Beyond this holding, it is the concurring opinions in *Jones*, by Justices Sotomayor and Alito, which offer further explanation of the unique issues attending location data, a reasonable expectation in privacy, and the third-party doctrine.[99]

Justice Sotomayor's concern is with a person's reasonable expectation of privacy in the intimate details of life revealed by location data. Her concurrence notes the unique aspects of location monitoring, which, even in the short term, "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[100] Whether by a GPS device or by smartphone location data, the precision of

---

[93] *See id.* at 404, 409–10; Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[94] *See Jones*, 565 U.S. at 414–16 (Sotomayor, J., concurring); *see also Jones*, 565 U.S. at 424–25, 430 (Alito, J., concurring); *see also Carpenter*, 138 S. Ct. at 2220.

[95] *See Jones*, 565 U.S. at 402–03.

[96] *Id.* at 403.

[97] *Id.* at 404, 406–07.

[98] *Id.* at 404–05.

[99] *See id.* at 414–16 (Sotomayor, J., concurring) (warning that the majority's test will provide little guidance in "cases of electronic or other novel modes of surveillance"); *id.* at 424–25, 430 (Alito, J., concurring).

[100] *Id.* at 415 (Sotomayor, J., concurring).

location monitoring catalogues the habits and characteristics of an individual.[101] As Justice Sotomayor suggests, such a catalogue of location data may infringe an objective reasonable expectation of privacy.[102]

Justice Sotomayor's concurrence clarifies that any single public activity is not the problem, it is "whether people reasonably expect that their movements will be recorded and *aggregated* in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[103] The term aggregation implies that it is the comprehensive picture provided by location tracking and its accuracy in showing patterns of movement that matter: two things that geofence warrants do exceptionally well. Location data has become a retrospective, unerring, and complete surveillance that outmatches other forms of surveillance in scope and complexity.[104]

The depth of these issues led Justice Sotomayor to suggest it "may be necessary to reconsider the premise" behind the third-party doctrine.[105] Calling the doctrine "ill suited to the digital age," her concurrence stresses that data is relayed to third parties in mundane, casual circumstances and thus she "would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[106]

Justice Alito also filed a concurrence that the government's actions amounted to a search, but largely because of the reasonable expectation of privacy a person has against the *long-term* tracking of their movements.[107] His concurrence focuses on what he considers the actual important issue, namely "the use of a GPS for the purpose of long-term tracking" and disagrees with the majority opinion that a minor trespass is what triggers Fourth Amendment protection.[108] Although Alito critiques the majority's opinion on multiple points, the most relevant here is his concern that electronic surveillance can "make long-term monitoring relatively easy and cheap."[109] Given that this ability is a novel, high-tech problem without a current legislative fix, applying "existing Fourth Amendment doctrine" is the best that can be done as a stopgap.[110] For Alito, short-term monitoring in public areas does not infringe a reasonable expectation of privacy. A focus on short-term public monitoring contrasts with geofence warrants, which can easily enter private areas, into the confines of the home, showing a pattern of movement from room to room.

---

[101] *See supra* Section I.B.

[102] *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

[103] *Id.* at 416 (Sotomayor, J., concurring) (emphasis added).

[104] *Id.* at 415–16 (noting that GPS monitoring is cheap, easily stored, and can be mined for years).

[105] *Id.* at 417.

[106] *Id.* at 417–18.

[107] *See id.* at 420–21, 424–25, 429–30 (Alito, J., concurring).

[108] *Id.* at 424–25 (emphasis omitted).

[109] *Jones*, 565 U.S. at 429 (Alito, J., concurring).

[110] *Id.* at 430.

Both Justices Sotomayor and Alito's concurrences utilize the *Katz* reasonable expectation of privacy test.[111] Justice Sotomayor focuses on the aggregation of data, which can show a comprehensive picture of an individual, emphasizing what is seen in the data rather than the length of location tracking.[112] She likewise questions the continued validity of the third-party doctrine, where users can agree to giving over vast amounts of data with one click. Alito, on the other hand, avoids any concerns with the third-party doctrine. Instead, to determine whether a reasonable expectation of privacy existed, Justice Alito focuses strongly on the length of public location tracking as a trigger to when a search occurs, with long-term public monitoring being more likely to be a search.[113] Justice Alito does not get specific as to what constitutes short-term versus long-term; at the very least, the GPS monitoring in *Jones*—twenty-eight days—satisfied 'long term.'[114]

Both concurrences apply squarely to the data of a geofence warrant. Both concurrences concern themselves with the relative ease with which law enforcement can obtain a complete surveillance of an individual,[115] which is a design feature of the location data in geofence warrants. Geofence warrant location data can be extremely detailed, offering a comprehensive picture of a person's activities for long periods of time. But neither concurrence says how much is too much, either in an aggregate picture of an individual or in the length of time that they have been tracked. Thus, it seems that these concerns must be approached on an ad hoc basis, both for courts and law enforcement. Less location data observed (both in a length of time sense and in a private area sense) will generally favor the government that a search has not occurred, and greater amounts of location data observed will generally favor a defendant's argument that a search occurred and a warrant was required.

The Court considered location data again in *Carpenter v. United States*, re-emphasizing many of the points raised in *Jones*. In *Carpenter*, wireless carrier providers handed over location data to the government by means of a court order rather than a search warrant.[116] The data implicated one of the defendants, Carpenter, in a series of robberies.[117]

The location data consisted of a time-stamped record of the phone's location, known as cell-site location information, or CSLI, automatically generated for the provider's business purposes.[118] The court orders sought four months' worth of CSLI which provided "12,898 location points cataloging Carpenter's movements" during

---

[111] *See id.* at 414, 416 (Sotomayor, J., concurring); *id.* at 419, 422–23 (Alito, J., concurring).

[112] *See id.* at 416 (Sotomayor, J., concurring).

[113] *Id.* at 430 (Alito, J., concurring).

[114] *Id.*

[115] *See* Jones, 565 U.S. at 415–16 (Sotomayor, J., concurring); *see also id.* at 428–29 (Alito, J., concurring).

[116] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

[117] *Id.* at 2212–13.

[118] *See id.* at 2211–12.

the string of robberies.[119] Carpenter argued that the seizure of the CSLI without a warrant violated the Fourth Amendment.[120] On appeal to the Sixth Circuit, the court there concluded that the detailed location information provided to the government was mere routing information provided to a third party; and as such, the third-party doctrine saw such routing information as a business record, to which a user had no reasonable expectation of privacy.[121]

In reviewing the Sixth Circuit's decision, the Court relied on *Jones* and distinguished the third-party doctrine. In essence, the majority holding, written by Chief Justice Roberts, fused some elements from both concurrences in *Jones*.[122] Chief Justice Roberts stressed that "[m]apping a cell phone's location over the course of 127 days provide[d] an all-encompassing record of the holder's whereabouts" which revealed "not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[123] Here, crucially, both the length of time and the patterns it demonstrated to the government would violate a reasonable expectation of privacy, triggering a search.

The Court determined that a phone's "exhaustive chronicle of location information"[124] is distinguishable from that early line of cases that established the third-party doctrine.[125] In distinguishing location data from other business records invoked by the third-party doctrine, the Court recognized that cell phones have become "almost a 'feature of human anatomy' . . . track[ing] nearly exactly the movements of its owner."[126] Further, tracking by CSLI occurs before the government even knows which suspect they intend to seek out. For CSLI, the data is transmitted to the phone provider whenever the phone is on and provides a faithful record of the activities of that individual, far before the government even knows they need it.[127] And CSLI implicates a vast number of individuals, as the Court noted, "location information is continually logged for all of the 400 million devices in the United States . . . ."[128] Therefore, relying on *Jones* and distinguishing earlier cases of the third-party doctrine, the Court held that a user "maintains a legitimate expectation of privacy in the record

---

[119] *Id.* at 2212.

[120] *Id.*

[121] United States v. Carpenter, 819 F.3d 880, 886–87 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206 (2018).

[122] *See Carpenter*, 138 S. Ct. at 2217 (highlighting both the "127 days" of location tracking and how it revealed "an intimate window into a person's life" and citing Justice Sotomayor's concurrence in *Jones*).

[123] *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[124] *Id.* at 2210.

[125] *Id.* at 2217 ("[W]hen *Smith* was decided in 1979, few could have imagined . . . a phone go[ing] wherever its owner goes, conveying . . . a detailed and comprehensive record of the person's movements.").

[126] *Id.* at 2218.

[127] *See id.* at 2211, 2218.

[128] *Id.* at 2218.

of his physical movements as captured through CSLI"[129] and to retrieve at least seven days of CSLI records from a wireless carrier, the government needs a warrant.[130]

The parallels between CSLI and the location data of a geofence warrant show why a party should normally have the same reasonable expectation of privacy in both, but primarily because CSLI and geofence location data both reflect twin concerns of *Jones* emphasized in *Carpenter*: a long-term picture of expressive public movements. As for parallels, CSLI is transmitted just by merit of having a connection to a cell tower, and the location data in a geofence warrant is transmitted once a user has opted in to Google's location services. For the latter, the phone's precise movement is logged so long as location and data are enabled, which can provide an extremely detailed picture of movement over time.[131] And while Google has begun to take steps to automatically delete location data, that near perfect record is stored by default for eighteen months on Google servers.[132] Further, just like CSLI, the movement patterns accumulated by a company like Google implicate a significant portion of the population. Precise numbers are unknown because much of the functionality of Google location services is proprietary, but at least one billion individuals globally use Google Maps every month.[133]

Chief Justice Roberts stressed *Carpenter* as a narrow holding,[134] but the 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 that case. For example, in writing for the majority, Chief Justice Roberts casts the constant record-keeping of CSLI data as "tireless and absolute surveillance"[135] and phone companies as witnesses "ever alert, and their memory [] nearly infallible."[136] The opinion characterizes long-term location tracking as "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[137] The location

---

[129] *Id.* at 2217.

[130] *See id.* at 2206, 2217 n.3.

[131] *See supra* Section I.B.

[132] Jessica Bursztynsky, *Google Just Announced It Will Automatically Delete Your Location History by Default*, CNBC (June 24, 2020, 12:00 PM), https://www.cnbc.com/2020/06/24/google-will-automatically-delete-location-history-by-default.html [https://perma.cc/K6BD-HSW2].

[133] Ethan Russell, *9 Things to Know About Google's Maps Data: Beyond the Map*, GOOGLE CLOUD BLOG (Sept. 30, 2019), https://cloud.google.com/blog/products/maps-platform/9-things-know-about-googles-maps-data-beyond-map [https://perma.cc/8Y5Z-6D4F]. Assumedly, only some subset of those one billion are American citizens, but this still implicates a large portion of the U.S. population.

[134] *Carpenter*, 138 S. Ct. at 2220 (2018) ("Our decision today is a narrow one. . . . We do not . . . address other business records that might incidentally reveal location information."). It is important to note that the movement patterns obtained by companies like Google are not obtained "incidentally."

[135] *Id.* at 2218.

[136] *Id.* at 2219.

[137] *See id.* at 2220.

data in a geofence warrant shares these concerns, irrespective of how Google Location History is initially obtained by consent or for how long it is retained.

The words tireless, absolute, ever alert, or infallible are not chosen idly to describe CSLI data. They are chosen to emphasize that society would likely find the details in CSLI data too invasive, harming an objective privacy interest.[138] Geofence location data is more invasive because of its increased accuracy and easy, cheap capacity to be retroactively searched.

A question remains as to how the concepts of time and accuracy overlap. Chief Justice Roberts' opinion indicates that the length of time that a person is tracked is worrisome: the Court here arbitrarily chooses seven days as too long,[139] which suggests that a longer time is worse, all things equal. Justice Alito stressed this view in *Jones*, which seems to make sense because it necessarily means that a greater overall picture of the user is obtained.[140] But at what point does the accuracy of the tracking surpass the length of time as the measure of objective reasonableness? What accurate form of location data could be too invasive for *any* period of time? For example, consider that location data can easily follow an individual into areas nominally considered some of the most private and intimate, areas that the Court has previously afforded an impressive amount of protection.[141] Even a geofence warrant that limits itself to a single day could follow a person from the interior of their home, among the rooms of their dwelling, to the location of a crime, then to a place of worship, then perhaps to a new home, such as that of a relative or friend, and among the rooms of that second dwelling. This form of tracking should likely constitute a search, for it invades so many places previously given so much Fourth Amendment protection.

For the reasons described in the concurrences in *Jones* and the majority in *Carpenter*, 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. At the very least, per *Carpenter*, *long-term* is any capture beyond seven days. Beyond that, what constitutes *long-term* versus *short-term* is unclear, and the permissible capture of location data for a short period of time might be inversely correlated with how detailed the location data is: where the accuracy of location data is very high, the permissible window of short-term capture of location

---

[138] *See id.* at 2217.

[139] The majority's holding stated it is "sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a . . . search." *Id.* at 2217, n.3. But the expressive language highlighting the danger of location tracking considered all the government's actions, which included an order for location data spanning 127 days. *Id.* at 2217.

[140] The majority opinion in *Carpenter* did not suggest that a certain distance traveled by the suspect suddenly triggered greater privacy, but that the overall record formed an "intimate window into a person's life." *Id.* at 2217. Nonetheless, location data records are formed based on length of capture anyway, with a greater distance of travel likely occurring dependent on the time requested.

[141] *See* Kyllo v. United States, 533 U.S. 27, 38–41 (2001) (through the wall infrared thermal surveillance of home without a warrant found to be unconstitutional).

data is very narrow. Further, location data may be determined to be so invasive within intimate areas that any amount of capture without a warrant is unreasonable.

B. Location Data as "Content" Under the Stored Communications Act

Independent of the analysis raised by the principle of *Katz* and the analysis in *Jones* and *Carpenter*, a statutory framework is implicated here. The Stored Communications Act (SCA), passed in 1986, regulates, among other things, the conduct of government actors in requesting or compelling network service providers to disclose stored communications.[142] In the statutory text, the SCA draws a distinction between different services provided,[143] a distinction that is now mostly eclipsed by an interpretation of the SCA's distinction between content and non-content information.[144] In very simple terms, the focus is often whether a government actor seeks the contents of an electronic communication, held by an electronic communications service. If so, the SCA requires the government obtain a warrant.[145] Reflecting that focus, if the location data within a geofence warrant is interpreted by a court as content data, a warrant is required. This is true independent of the analysis of location data invoked by *Katz*, *Jones*, and *Carpenter*.

Notably, Google, as *amici* in *United States v. Chatrie*, takes the position that location data is content and does require a warrant under the SCA.[146] The SCA defines content as a part of an electronic communication which concerns "the substance, purport, or meaning of that communication."[147] Applying this definition

---

[142] 18 U.S.C. § 2703; *see also* Melissa Medina, Note, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 277 (2013). The SCA shows its age in colorful ways, reserving a whole section for a private right of action against the wrongful disclosure of video tape rental or sale records. 18 U.S.C. § 2710.

[143] The SCA distinguishes between an electronic communications system (ECS) and a remote computing service (RCS) in a manner reflecting the electronic landscape of 1986, unhelpful to modern ISP practices, where ISPs often perform both tasks. An ECS means a provision "to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). An RCS is the "provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

[144] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("[T]o the extent that the SCA purports to permit the government to obtain [the contents of] emails warrantlessly, the SCA is unconstitutional.").

[145] United States v. Graham, 824 F.3d 421, 437 (4th Cir. 2016) (en banc), *abrogated by Carpenter*, 138 S. Ct. 2206.

[146] Google Amicus Brief, *supra* note 22, at 16 ("Google [Location History] information is subject to the SCA's warrant requirement because that information qualifies as 'contents' of 'electronic communications.'").

[147] 18 U.S.C. § 2510(8). "Electronic communication" itself has a very broad definition, including in part "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire." § 2510(12). This does not include a "tracking device" defined as "an electronic or mechanical device which permits the tracking

to the location data as used by Google users, Google argues that "[t]he user's location itself is the 'substance' and 'meaning' of the data the user transfers to Google."[148] Because it is a recording of movements, chosen by the user to be logged, "capable of being reviewed, edited, and deleted by the user[,]" it is content more akin to a journal or itinerary.[149] Of course, it is in Google's interest to interpret it this way, given it is their resources that are subject to query and search, and a different interpretation could leave them subject to an even greater number of legal requests short of warrants.

Google could have a point, irrespective of their interests. The analysis of whether location data is content is relative to how it is used, and an analogy in these types of questions of content versus non-content is compelling:

> [T]he line between content and non-content information is inherently relative. If A sends a letter to B, asking him to deliver a package to C at a particular address, the contents of that letter are contents from A to B but mere non-content addressing information with respect to the delivery of the package to C.[150]

Location data often can be incidental to the transmission of the information itself, as in *Carpenter* where CSLI data was captured merely "by dint of its operation,"[151] or as more akin to header information that gets it from one place to another.

For geofence warrants, there is no incidental capture or mere addressing information. A user opts into this service to use for their own purposes. In this instance, Location History data is sent to Google's servers not as an incidental metric or as header/addressing information helping it to be routed correctly, but instead to be logged for purposes unto itself. Google, as *amici*, stresses this point that the location data is, itself, substantive as conveyed,[152] implying that Google is to utilize the data as is not only for targeted advertising but also as a service for the consumer, for example, as a recorded log or journal of movement patterns in the Google Maps service.

Prior to *Carpenter*, some courts had concluded that location data, in the form of CSLI, was not content under the SCA and could be obtained by an order under Section 2703(d) of the SCA, which does not require probable cause.[153] Now, without

---

of the movement of a person or object." § 3117(b). It is very unclear whether this "tracking device" definition, unaltered since 1986, is strictly limited to devices whose singular purpose is to track location or instead to devices that track location and also do other things.

[148] Google Amicus Brief, *supra* note 22, at 16.

[149] *Id.*

[150] 2 WAYNE LAFAVE ET AL., CRIMINAL PROCEDURE § 4.4(d), at 461–62 (3d ed. 2007); *see also In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 136–37 (3d Cir. 2015) (employing this analogy in its analysis).

[151] *See* Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

[152] Google Amicus Brief, *supra* note 22, at 17.

[153] *See, e.g.*, *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).

directly ruling on whether location data is now considered content, those same courts are compelled by *Carpenter*'s holding to the opposite conclusion: a Section 2703(d) order cannot be used to obtain CSLI location data because it requires less than probable cause.[154] This about face, brought on by *Carpenter*, suggests that Google's *amici* brief may be compelling, but not for the reasons it suggests. Google suggests that because a user can catalogue expressive activity as a substantive record held by a third party, anything like that should be designated as a content record.[155] So, because location data is such an expressive, substantive record, it is content too. Perhaps it is simpler than that; *Carpenter*'s holding renders location data subject to a reasonable expectation of privacy and holding otherwise under the SCA's terms would simply create an incongruity that the courts cannot permit. So, regardless of the actual answer as to whether location data is or is not content, some courts have rejected the government's mere use of an SCA court order to obtain location data,[156] and so the finding related to *Jones* and *Carpenter* likely controls.

III. GEOFENCE WARRANT REQUIREMENTS

Part II argued that a request for location data from a third party constitutes a search and thus requires a warrant. Assuming that point for the sake of further analysis, Part III continues to identify and grapple with the primary issues that arise with a geofence warrant, focusing on the probable cause and particularity requirements. This analysis relies primarily on publicly available geofence search warrant applications and those very few district court cases which have analyzed these issues in geofence warrants.

Generally, the warrant framework is as follows: "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few . . . exceptions."[157] So, without a valid exception, a search requires a warrant issued by a "neutral and detached magistrate" who independently verifies that the warrant satisfies Fourth Amendment requirements.[158] The first primary requirement for the issuing magistrate is to determine that the warrant is supported by probable cause,[159] a task the Supreme Court has labeled a "practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . , there is a fair probability that contraband or evidence

---

[154] *See, e.g.*, United States v. Goldstein, 914 F.3d 200 (3d Cir. 2019).

[155] Google Amicus Brief, *supra* note 22, at 6–9.

[156] *See, e.g.*, *id.*

[157] Katz v. United States, 389 U.S. 347, 357 (1967). The many exceptions to the warrant requirement are not directly addressed in this Note, which instead focuses on the requirements of probable cause and particularity.

[158] Johnson v. United States, 333 U.S. 10, 14 (1948).

[159] U.S. CONST. amend. IV ("[A]nd no Warrants shall issue, but upon probable cause . . . ."). The application for a search warrant must be sworn out by oath or affirmation. *Id.*

of a crime will be found in a particular place."[160] Another primary requirement is that the warrant "particularly describ[e]" the place, person, or thing subject to search or seizure,[161] which "makes general searches under [a warrant] impossible[,] . . . [leaving nothing] to the discretion of the officer executing the warrant."[162] This particularity requirement fulfills the "objective . . . that those searches deemed necessary should be as limited as possible."[163]

In focusing on what satisfies probable cause and particularity, a court aims toward what is *reasonable* in those regards. If we keep that in mind, the conclusions of Part III are relatively straightforward. For probable cause, it is more reasonable to assume that evidence of a crime will be found in location data where the police have established a narrow and objectively limited warrant: a warrant with a high probability of capturing the data of those for whom probable cause has been established. Therefore, warrants that are overbroad and capture the location data of many uninvolved individuals suffer from probable cause issues. For particularity, discretion is limited where the police draw multiple *ex ante* geofence targets, restricting the search to the initial terms of the warrant, rather than permitting any *ex post* sorting procedure of the warrant returns thus reasonably avoiding the hated general warrants of the past. Geofence warrants adhering to these ideas are more likely to be constitutionally valid than those that do not.

A. Geofence Warrants: How to Satisfy Probable Cause

In general, probable cause "does not demand the certainty . . . associate[d] with formal trials."[164] It is a "flexible, common-sense standard" expecting a reasonable belief that contraband or evidence of a crime will be found in the person, place, or thing searched or seized.[165] "[I]t does not demand any showing that such a belief be correct or more likely true than false."[166] What it does demand is "some quantum of individualized suspicion" that suggests the person being searched is unlike those not subject to a search.[167] With such a flexible standard, however, a great amount of deference is afforded to law enforcement and magistrate judges making probable cause determinations.[168] Practically speaking, probable cause is established by facts

---

[160] Illinois v. Gates, 462 U.S. 213, 238 (1983).

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

[162] Stanford v. Texas, 379 U.S. 476, 485 (1965) (quoting Marron v. United States, 275 U.S. 192, 196 (1927)).

[163] Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

[164] *Gates*, 462 U.S. at 246.

[165] Texas v. Brown, 460 U.S. 730, 742 (1983).

[166] *Id.*

[167] United States v. Martinez-Fuerte, 428 U.S. 543, 560 (1976); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (quoting *Martinez-Fuerte*, 428 U.S. at 560).

[168] *See* United States v. Leon, 468 U.S. 897, 914 (1984) ("Reasonable minds frequently

established before the warrant is filed, and those facts are derived from, among other things, observation, independent sources, or previously seized evidence.[169] As it pertains to geofence warrants, probable cause requires that evidence of the offense under investigation will be found on the servers of the company from whom geolocation data is requested. Police can potentially rely on the practical methods outlined above to establish that relation. For example, some available probable cause affidavits (filed in support of geofence search warrant applications) rely strongly on a form of observation, either from video surveillance[170] or from eyewitness observation,[171] to tie an unknown suspect to a crime.

In the most convincing probable cause affidavits, the established facts typically proceed as follows. They begin by identifying some set of facts that indicate the commission of a crime, an unknown suspect observed around the location of the crime, and, crucially, an observer that saw the unknown suspect use a cell phone near the location of the crime.[172] At this point, the warrant typically generalizes, with the affiant establishing their expertise and describing the general features of cell phones, the capability of some cell phones to pinpoint location, that Android devices usually have related Google accounts, that Google accounts with location services enabled may have that data stored on Google's servers, and that the observed phone could have such data.[173]

---

may differ on the question whether a particular affidavit establishes probable cause, and we have thus concluded that the preference for warrants is most appropriately effectuated by according 'great deference' to a magistrate's determination.") (quoting Spinelli v. United States, 393 U.S. 410, 419 (1969)); *see also* Erica Goldberg, *Getting Beyond Intuition in the Probable Cause Inquiry*, 17 LEWIS & CLARK L. REV. 789, 800–03 (2013).

[169] *See* McDonald v. United States, 335 U.S. 451, 454–55 (1948) (observation); *see also Gates*, 462 U.S. at 237–38 (anonymous informant); United States v. Sharpe, 470 U.S. 675, 682–83 (1985) (lawful seizure).

[170] *See* Application for Search Warrant, *In re* accounts associated with the area near the location 35.785556°, -78.617145° between 6:00pm EST and 7:00pm EST on 11-07-2016, and Between 5:25pm EST and 6:25pm EST on 11-08-2016, Maintained on Computer Servers Controlled by Google, Inc. (N.C. Super. Ct. Mar. 8, 2017) [hereinafter March 8, 2017 Geofence Warrant], https://www.documentcloud.org/documents/4388571-20170308-homicide-warrant.html#document/p5/a410668 (relying on video surveillance footage of a suspect).

[171] Application for Search Warrant, *In re* Accounts associated with the area near the location 35.833966°, -78.609595° Between 3:00am EST and 4:00am EST, on 06-01-2015, Maintained on Computer Servers Controlled by Google, Inc. (N.C. Super. Ct. Mar. 7, 2017) [hereinafter March 7, 2017 Geofence Warrant], https://www.documentcloud.org/documents/4388570-20170307-homicide-warrant.html#document/p6/a410393 (relying on an eyewitness account of a suspect).

[172] *See id.* at Attachment III ("One witness watched as the unknown suspect used the light from his cellular phone to either light a path to a vehicle or look for something on the ground."); *see also* March 8, 2017 Geofence Warrant, *supra* note 170, at Attachment III ("The subject has a CELLULAR DEVICE in his left hand that is positioned near his left ear.") (alteration in original).

[173] *See, e.g.*, March 7, 2017 Geofence Warrant, *supra* note 171, at Attachment III (offering these expert generalizations in turn).

There is a step-by-step logic present here: an unknown suspect committed a crime, an officer or witness observed a suspect with a cell phone near the commission of that crime, and, if it is an Android device, Google may have location data about that device and thus evidence of the crime. Given the deferential standard of probable cause, one could be excused for assuming probable cause on that logic alone, as there is a good probability evidence of the crime could be there. But one would miss what is really being asked in the query demanded of Google. The SensorVault query, focused on a geofence location, will search *all* Android devices with stored location history for the corresponding GPS coordinates.[174] Beyond this, all Android users (with Location History enabled) within those boundaries will be returned by the warrant, but the affidavit will have provided for only *one* of those users, the attendant facts linking his cell phone use to the crime and thus potential evidence of the crime to Google's servers. Probable cause may exist for that single suspect, but it is harder to say that probable cause exists for all the other users swept up into the warrant returns because no facts are established to state they are involved in the crime.

There are instances where the link between the crime and Google's servers is even more attenuated. Other affidavits omit the observation of the suspect's cell phone—or even the suspect altogether—that was present in the last example. These other affidavits provide facts that suggest the commission of a crime. But these affidavits lack observation, or any comparable circumstantial evidence, that suggest the specific, unknown suspect that may have committed the crime *had a cell phone* on them at or near the commission of the crime.[175] Instead, these affidavits skip the observation that existed in the last example and instead rely solely on the expert generalizations about cell phones, location data, Android, and Google.[176] In these instances, there is a complete lack of connection between the historical facts upon which the warrant is based and hypothetical evidence on Google's servers. It is instead assumed that because of the ubiquity of cell phone use and the widespread market share held by Android devices, there is a high probability of obtaining evidence of the crime.[177] Even if, for the sake of argument, it is assumed as true that there is a high probability the suspect has a cell phone, the original issue is also still present: there might not be probable cause for all the other users swept up into the returns.

Because this technology is still new, case law analyzing this probable cause issue for geofence warrants is sparse. Two district court opinions, both from the Seventh

---

[174] Google Amicus Brief, *supra* note 22, at 12–13 ("Google must search across *all* [Location History] journal entries to identify users with potentially responsive [Location History] data . . . .") (emphasis added).

[175] *See* Application for Search Warrant, No. 27-CR-CV-18-4 (Minn. Dist. Ct. Oct. 8, 2018), https://www.documentcloud.org/documents/5729046-Google-Reverse-Search-Warrant-Eden-Prairie-Home.html; Raleigh Devices Geofence Warrant, *supra* note 14.

[176] *See, e.g.*, Raleigh Devices Geofence Warrant, *supra* note 14, at Attachment III (describing a suspected arson and mentioning nothing about a suspect's cell phone use before then generalizing about cell phones and cell phone use).

[177] *See, e.g.*, *id.*

Circuit, demonstrate rationales for either refuting a finding of probable cause or accepting a finding of probable cause.

In the first case, referred to here as the "pharmaceuticals case," the government sought a geofence warrant for an unknown suspect who received stolen pharmaceuticals within the area outlined by the affidavit.[178] After a point on warrant protocol,[179] the district court began by emphasizing the scope of the warrant: "a form of authority . . . disclos[ing] . . . the identities of various persons whose Google-connected devices entered the geofences[.]"[180] While the court acknowledged the "fair probability" that the unknown suspect and evidence of the crime would be on Google's servers, "the proposed geofence warrant will [also] *include* the precise geographic location of persons as to whom no showing has been made as to their involvement in the offense or with the [u]nknown [suspect]."[181] Instead, these persons and their data are involved with the warrant by their proximity alone, that is, just "because those users were found in the place to be searched."[182] Ultimately, the district court's probable cause analysis relied on U.S. Supreme Court precedent previously rejecting a similar argument.[183] In that case, *Ybarra v. Illinois*, the Court concluded that an unrelated person's mere proximity to a suspect for whom probable cause has been established is insufficient on its own.[184] Instead, the Court noted that:

> Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person. This requirement cannot be undercut or

---

[178] Applicant for Search Warrant, *In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 U.S. Dist. LEXIS 165185 (N.D. Ill. July 8, 2020) [hereinafter *Google I*] (application initially denied on particularity grounds). The probable cause analysis was taken up again in *In re* the Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 749–50 (N.D. Ill. 2020) [hereinafter *Google II*].

[179] In a point on protocol, the district court found no difference between two forms of geofence warrant proposed by the government. *Google II*, 481 F. Supp. 3d at 749. The first is retrieving anonymized returns that could then, on the authority of the same warrant, be compelled into a narrower set of non-anonymized returns. *Id.* The second is a warrant that would only provide anonymized returns. *Id.* For the second type, the government would then need to seek further court process to turn the anonymized returns into intelligible subscriber information. *Id.* Crucially, because *both* types "could be construed by Google to include *all* of the devices captured within the geofences[,]" they would render the same results in the anonymized first step between either type. *Id.* at 750. Thus, the second step—either by the authority of the initial warrant, or a follow-up subpoena—is identical in substance, if not form, because both are so easily obtained. *Id.* Concerned over the liberty interest already invoked in the first step, the court determined that both types must meet Fourth Amendment principles. *Id.*

[180] *Id.* at 750–51.

[181] *Id.* at 751.

[182] *Id.*

[183] *See* Ybarra v. Illinois, 444 U.S. 85, 90–92 (1979) (holding that a valid warrant with good probable cause for a bar and bartender did not extend to a patron who was on the premises).

[184] *See id.* at 91.

> avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be.[185]

The district court found probable cause lacking for similar reasons, as a number of Google users would be included in the geofence warrant returns because they happened to be nearby.[186] Their sweep into the warrant was coincidental, purely based on spatial relation. If this reasoning regarding *Ybarra* is accepted, it could be applicable to geofence warrants in two categories: those broadly drawn by scale and duration (implicating many by geography and time) and urban geofence warrants (where the density of users is simply much higher). Most geofence warrants, but especially those that are broad or urban,[187] will sweep up into the warrant returns numerous bystanders who will have had no rational connection to the crime, even as witnesses. The main distinguishing feature between *Ybarra*'s facts and geofence warrants generally is the physicality of the search. In *Ybarra*, the police physically searched a person within the boundaries of the warrant.[188] Geofence warrants involve a person's things (data), held by a third party on a computer server, and analyzed after the fact to see whether the data is really related to a crime or not. It is unclear whether this distinction, tangible and present versus intangible and distant, would make a difference to a court.[189]

In the second case, referred to here as the "arson case," the government sought a geofence warrant which sought arson suspects over six target locations.[190] Unlike the pharmaceuticals case, where the geographic boundaries were in a dense, urban area, the target locations in this case were drawn over more sparse areas, both private and public, including commercial lots, which included company infrastructure, and a public street and alleyway.[191]

Further, unlike the pharmaceuticals case, here the district court found that probable cause was present.[192] To understand why, it is important to note that in both cases

---

[185] *Id.*

[186] *Google II*, 481 F. Supp. 3d at 753 ("Because the proposed warrant here seeks information on persons based on nothing other than their close proximity . . . , the Court cannot conclude that there is probable cause to believe that the location and identifying information of any of these *other* persons contains evidence of the offense.").

[187] *See id.* at 752 (noting that the geofence warrant returns would include any sidewalk passersby, retail customers in an adjoining business and parking lot, drivers on a nearby street, and persons in residential units).

[188] *See Ybarra*, 444 U.S. at 88–89 (discussing that Ybarra was twice patted down, and on the second, a cigarette pack containing heroin was removed from his pants pocket).

[189] It did not matter to the district court, who considered the distinction a simple analogy. *See Google II*, 481 F. Supp. 3d at 753.

[190] *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 351 (N.D. Ill. 2020). Some of the targets were identical in space but set at a different time. *Id.* at 352–53.

[191] *See id.* at 351–53.

[192] *Id.* at 354.

no suspect was observed using a cell phone during the commission of the crime.[193] This is unlike those ideal affidavits outlined above where a witness or surveillance system observed that the suspect had a cell phone. Instead, the district court in the arson case relied on the affiant's training and experience and "several statements supporting probable cause that evidence of the crime would be located at Google."[194]

The affiant, an Alcohol, Tobacco, Firearms and Explosives agent, noted that based on his training and experience, it was common for co-conspirators to use cell phones to plan and commit certain crimes, especially when the same crime (like arson) occurs on separate dates.[195] Further, there is "a reasonable probability that a cell phone, regardless of its make, is interfacing in some manner with a Google application, service, or platform."[196] And "anyone passing near or through the target locations . . . could be perpetrators or witnesses to the arsons."[197] The district court found probable cause, relying on circuit precedent establishing that the statements of experts can suffice to establish probable cause,[198] the ubiquity of cell phone use, the high likelihood of Google's overlap with most cell phones, and the common pattern of crimes like arson. These statements, even if accurate, are generalizations based the common aspects of a type of crime.

In addressing the argument that other Google users, neither suspect nor witness, could be included in the warrant returns by being present within the boundaries of the target location, the district court did not include its reasoning as part of its probable cause analysis.[199] The district court noted that the privacy concerns of uninvolved individuals are often indirectly impacted by a search, as when the search of a house involves occupants not suspected of a crime.[200] Or when an email account or cell phone, searched for evidence of a crime, reveals the intimate details of all those who messaged or interacted with the inbox or cell line.[201]

The district court focused on one point to avoid an issue with the other Google users implicated by a geofence warrant: "[t]he proper line of inquiry is not whether a search of location data could impact even one uninvolved person's privacy interest,

---

[193] *See id.* at 355 ("[I]t is important to note that there is no evidence in the affidavit that any of the suspects possessed cell phones or used cell phones in the commission of the offense."); *see also Google II*, 481 F. Supp. 3d at 732–33.

[194] *See In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d at 356.

[195] *Id.*

[196] *Id.*

[197] *Id.*

[198] *See id.* at 355–56.

[199] *See In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d at 359, 361 (including it under the subheading "Additional Considerations").

[200] *Id.* at 361 (noting that this indirect impact "is present in numerous other situations and is not unusual").

[201] *Id.*

but rather the reasonableness of the search, the probability of finding evidence at the location, and the particularity of the search request."[202] That probable cause is found for the unknown suspect is sufficient, so long as reasonableness and particularity are also found. In literal terms, a search on Google's servers has begun and ended when all users whose data matches given warrant parameters are reflected in the returns. Under the district court's reasoning, those other users whose data is incidentally searched simultaneously to the suspect's reflects common practice in warrants, and because common, an acceptable practice too.

The district court distinguishes *Ybarra* in a footnote, dispensing with the case, but perhaps also giving away what really makes the difference between the arson case and the pharmaceutical case.[203] It is noted that "the government is not expanding the scope of the warrant because it *explicitly* seeks location data for all individuals present in the geofence within the scope of the warrant."[204] So, everyone within the boundaries of the warrant can have their data searched, useful or otherwise, because the government explicitly targeted all of them and probable cause is satisfied for all of them.[205]

Because all of the individuals in one instance (the arson case) may be searched and they may not be searched in the other instance (the pharmaceutical case), the answer likely then turns on the *reasonableness* of the warrant application. In the pharmaceutical case, it seems unlikely that the claim could be made that because the government explicitly targeted an area and established probable cause as to a few individuals, all individuals there could be searched. The reason it is unlikely is because, in actuality, it would have potentially implicated the data of *hundreds* of individuals.[206] It is no stretch of the imagination to state that in a dense urban location, even a narrowly drawn geofence could implicate thousands of individuals if the time frame is sufficiently long. In the arson case, the target locations are lightly traveled, largely empty, commercial lots where suspicious fires have been set.[207] There are roadways and alleyways that the suspects may have used to travel either to or from the arson.[208] There are private buildings, but they are of mixed commercial use or garages.[209] Although public and private lands are involved, the implication in the district court's manner

---

[202] *Id.* at 362.

[203] *Id.* at 362 n.6.

[204] *Id.*

[205] *See In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d at 362 n.6. In *Ybarra*, would the government have received their warrant to search everyone on the tavern's premises if they had simply known a crime had occurred and—relying on their expertise alone—generalized about surrounding individuals from there? *But cf.* 444 U.S. 85, 90–92 (1979).

[206] *See Google II*, 481 F. Supp. 3d at 752 (noting that the proposed government warrant would capture location information of a vast number of individuals in the urban location).

[207] *See In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d at 351–53.

[208] *Id.* at 352.

[209] *Id.*

of speaking is that *very few* uninvolved users will be present in these warrants.[210] Indeed, the district court in the arson case notes that "there is no way to exclude the possibility that at any given time" an uninvolved Google user—for whom probable cause could never be established—would not wander through the geofence boundaries.[211] But when that possibility of uninvolved Google users is a near certainty, especially if it is certain that there will be hundreds of them implicated in the warrant—as was true in the pharmaceutical case—then the "finding of probable cause" for all of them is much less reasonable.

It is much more rational, then, to evaluate these opposite conclusions as to what a court considers reasonable.[212] Courts will find it easier to establish probable cause where the likelihood of incidentally searching other Google users is low,[213] because it is reasonable to assume that most of the Google users chosen are suspects, co-conspirators, or witnesses for which the government has supplied probable cause. So, geofence applications that focus on non-urban areas, or applications that are extremely tailored and narrowed by geographic and temporal scope will have a better chance of being accepted. Courts will struggle to grant a geofence warrant request where the likelihood of incidentally searching other Google users is high, because it is unreasonable to assume that probable cause extends to all of them.

B. Geofence Warrants: How to Satisfy Particularity

The text of the Fourth Amendment specifies that a warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized."[214] As the Supreme Court has explained, "[t]he manifest purpose of this particularity requirement was to prevent general searches . . . the requirement ensures that the search will be carefully tailored to its justifications . . . ."[215] Courts generally require that, to satisfy the particularity requirement, the warrant include: (1) the specific crime for which probable cause has been established; (2) the place to be searched; and (3) how the items relate to the specified crime.[216] This is relatively simple in terms of a physical search, where the description objectively narrows police officers to search those places where the evidence of the crime would be, and to avoid those places

---

[210] The district court's example of an uninvolved individual is a delivery truck driver entering the geofence location, but even then it is implied he could be a witness. *See id.* at 362.

[211] *Id.*

[212] *See* Florida v. Jimeno, 500 U.S. 248, 250 (1991) ("The touchstone of the Fourth Amendment is reasonableness." (citing Katz v. United States, 389 U.S. 347, 360 (1967))).

[213] *See, e.g.*, *Google I*, 2020 U.S. Dist. LEXIS 165185, at *14, n.8 (detailing with approval "a geofence warrant for an almost empty commercial parking lot where only one vehicle was located").

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

[215] Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[216] *See, e.g.*, United States v. Galpin, 720 F.3d 436, 445–46 (2d Cir. 2013).

where the evidence of the crime could not possibly be.[217] The most particular and satisfactory of warrants will leave nothing to the discretion of the person executing the warrant.[218]

It is easier said than done for courts to adapt the particularity requirement to digital contexts.[219] Professor Adam Gershowitz has noted "[t]here are two fairly narrow categories of cases in which courts tend to find particularity violations in computer search warrants."[220] A court will find a particularity violation where such a warrant does not properly "state on its face what crime the search is being conducted to find evidence of" and "when the search warrant contains overbroad, catch-all language."[221] The best likelihood for a defendant to succeed on a particularity issue regarding a computer search warrant is to identify these issues, but such challenges are "rarely successful."[222] So, a geofence warrant should, at a minimum: (1) describe the crime for which evidence is being sought; (2) describe where the data is being held; and (3) include specific language as to how the data relates to the crime.

When law enforcement is focusing on specific data intermingled among other data, rather than an object with a large storage capacity, the focus of the particularity requirement turns to "the content of the relevant files rather than on the storage devices which may happen to contain them."[223] As such, to avoid being overbroad, a warrant should describe and focus on the relevant files, if possible.[224] A specific way that courts have found data descriptions to be limited and focused is for officers to be clear about what they are seeking[225] and to restrict their search based on date

---

[217] *See Garrison*, 480 U.S. at 85 (noting that where officers would have known one apartment was a suspect's and one was an unrelated individual's, the particularity requirement obligates the officers to exclude the unrelated individual's apartment from their search).

[218] *See* Stanford v. Texas, 379 U.S. 476, 485 (1965).

[219] *See generally* Paul M. Ervasti, *Is the Particularity Requirement of the Fourth Amendment Particular Enough for Digital Evidence?*, ARMY LAW. (Oct. 2015), at 6–10 (describing some of the general difficulties related to digital evidence and the particularity requirement).

[220] Adam M. Gershowitz, *The Post*-Riley *Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 599 (2016).

[221] *Id.* at 599–600 (reviewing examples of courts sustaining particularity challenges in the described instances).

[222] *See id.* at 600.

[223] *Cf.* H. MARSHALL JARRETT ET AL., COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 72 (2009), https://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [https://perma.cc/JN5V-Y6U8] (citing United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009)).

[224] *See id.* (advising U.S. attorneys to "focus on the relevant files . . ." when the "computer is merely a storage device for evidence . . . .").

[225] *See* United States v. Burgess, 576 F.3d 1078, 1092 (10th Cir. 2009), *cert. denied*, 130 S. Ct. 1028 (2009); *see also* United States v. Adjani, 452 F.3d 1140, 1148 (9th Cir. 2006) (commenting favorably that a "warrant provided the 'precise identity' and nature of the items to be seized"), *cert. denied*, 549 U.S. 1025 (2006).

or time.[226] And, as was the case with probable cause, courts have found reason to be lenient. Some circuits have recognized that "'over-seizing' is an accepted reality in electronic searching because '[t]here is no way to be sure exactly what an electronic file contains without somehow examining its contents.'"[227]

In the few geofence warrant cases that have analyzed the issue of particularity, the warrant applications have failed the requirement if the discretion of the executing official is too broad.[228] As mentioned, it can be unconstitutional to permit the executing officer discretion in how the search will be conducted.[229]

Geofence warrant procedure often does permit a sort of impermissible discretion when officers are given anonymized returns from Google.[230] The reader will recall that, in either the case of a "multi-step" warrant or a warrant that then must be followed up with further legal process, Google produces anonymized device IDs in the warrant returns which the officers often sift through, picking and choosing which data can be attributed to suspect, witness, or non-witness.[231] Although the data is anonymized, the privacy of the data is not at issue; it is the fact that officers are sifting through the data at all. Particularity demands a specificity that, while not exactitude, leaves as little as possible for the officers conducting the search to decide to do.[232] Particularity has been found lacking in those instances where a geofence warrant simply provides "the executing officer unbridled discretion as to what device IDs" will be followed up on.[233] And, because many geofence warrants seem to rely on this procedure, many are likely unparticular in this regard, lacking the restrictions on police action necessary to satisfy the Fourth Amendment.

A court may come to a different result with the same warrant procedure but with different facts. But it is likely not the procedure of sorting that is suddenly permissible, but instead the low likelihood of actual discretion. For example, in the arson case, the district court found reasons to be lenient: the warrant was limited in time

---

[226] *See, e.g.*, United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995).

[227] United States v. Flores, 802 F.3d 1028, 1044–45 (9th Cir. 2015) (quoting United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam)).

[228] *See Google I*, 2020 U.S. Dist. LEXIS 165185, at *17 (N.D. Ill., July 8, 2020) (finding particularity unsatisfied because of a broad discretion left in sifting through anonymized warrant returns); *see also Google II*, 481 F. Supp. 3d at 754 (stating the warrant provides "unbridled discretion").

[229] *See* Stanford v. Texas, 379 U.S. 476, 485 (1965) ("[N]othing is left to the discretion of the officer executing the warrant." (quoting Marron v. United States, 275 U.S. 192, 196 (1927))).

[230] *See, e.g.*, Raleigh Devices Geofence Warrant, *supra* note 14, at Attachment I.

[231] *See id.* at Attachment 1 ("Law enforcement officers will *review* this 'anonymized information' provided by Google, Inc. in an effort to *narrow down* the list of accounts . . . .") (emphasis added).

[232] *See Google II*, 481 F. Supp. 3d at 754; *see also* United States v. Sanchez-Jara, 889 F.3d 418, 421 (7th Cir. 2018) (holding that a warrant that identified *ex ante* the phone to be tracked satisfied the particularity requirement), *cert. denied*, 139 S. Ct. 282 (2018).

[233] *See Google II*, 481 F. Supp. 3d at 754.

and location,[234] and also, it was limited in scope.[235] As for time and location, the court noted with satisfaction that the data would return the location patterns of those within the geographic boundaries for no longer than thirty-seven minutes.[236] Those locations themselves were at least implied to be limited,[237] expecting that there was likely to be few people there at all.[238] The court's discussion on the scope of the warrant arguably implicates the most important aspect as to why this warrant may satisfy the particularity requirement where others would not: "the geofence zones have been constructed to *focus on* the arson sites and the streets leading to and from those sites. Residences and commercial buildings along the streets have been *excluded* from the geofence zones."[239] The sifting procedure is not suddenly permissible; it is not likely to be used at all. Anyone found in these locations is likely a suspect or witness, and the officers will have no true discretion to sift among them.

As the court in the arson case found in relation to probable cause, the investigating agents took care, ex ante, to draw the geofence in a manner that implicated as few potential Google users as possible. Because this is a prospective limitation on the executing officer, it does act as an objective limitation on that officer's discretion, as does both the time and location limitations. But the scope limitation is arguably the most important because it recognizes and prevents what would truly perturb the court and its Fourth Amendment analysis: capturing the data of a wider swath of potential Google users who are almost both unrelated to the crime and who would be sorted. Because the investigating officers provided "support [to] the conclusion that location data from uninvolved individuals will be minimized," the warrant was limited in scope, and satisfied the particularity requirement.[240]

What general principles might satisfy particularity in those cases unlike the arson case, where the capture of other Google users cannot be avoided? One method suggests that the investigating officers draw multiple narrow and specific geofence targets and request Google to return device IDs for only those whose location data is found in all of the targets.[241] The logic here seems to easily conform to particularity

---

[234] *See In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F.3d at 357–58.

[235] *See id.* at 357–59.

[236] *See id.* at 357 (noting the longest period of time for the warrant is a thirty-seven-minute period for one of the target locations).

[237] *See id.* at 358 (noting the target areas are "drawn to capture location data from locations at or closely associated with the arson").

[238] *See id.*

[239] *Id.* (emphasis added).

[240] *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F.3d at 358.

[241] Magistrate Judge Weisman of the Northern District of Illinois developed this potential means of satisfying particularity in response to the denial of a geofence warrant; a favorable analysis of it was included in the pharmaceutical case, *Google II*. *See* 481 F. Supp. 3d at 755–56.

principles: these targets would be objective limitations, obtained in advance, for which the executing officers had no true discretion in sifting through. Further, "[t]he likelihood of the same device showing up in more than one of these [] geofences is extremely low . . ." which aids not only the particularity analysis, but the probable cause analysis as well.[242] So, for example, if it is known which route the suspect took and when he likely arrived, where and when the crime likely occurred, and then which route the suspect took and when he made his escape, a geofence warrant that sought location data on only those devices within all of those target locations, which themselves are properly restricted in scope, could likely satisfy particularity principles.

CONCLUSION

Geofence warrants present novel problems for the criminal justice system. These problems will not wait around for more extensive guidance; courts will face them more and more. A few conclusions can be suggested from what is currently known.

First, there are two conclusions regarding whether a warrant is required when executing a geofence warrant for location data. *Jones* and *Carpenter* treated location data as a unique thing which revealed intimate facts about a given individual. A majority in *Jones* and the Court's opinion in *Carpenter* found a reasonable expectation of privacy for location data in their respective cases. Because the location data in a geofence warrant is *more* precise, a similar reasonable expectation is very likely invoked, and a warrant is required. Independently, courts have interpreted that *Carpenter* has foreclosed the ability to obtain location data without a warrant under the Stored Communications Act. To permit otherwise would be incongruous with this Supreme Court precedent.

Second, consistent issues arise with regards to the probable cause and particularity requirements, especially overbreadth and impermissible discretion in the execution of the warrant. This Note ultimately concludes that law enforcement may rely upon usual methods to establish probable cause, using special caution to limit uninvolved users for whom probable cause cannot be obtained by drawing geofence warrants narrowly. Further, law enforcement can establish particularity with multiple geofence target locations, within which there is a high likelihood that the only recurring users are suspects or witnesses. This avoids the use of sorting procedures after the fact. The ideal application for a geofence warrant is one which increases the chances that *only* the suspect's data will be captured by the warrant. Courts view the Fourth Amendment requirements through the lens of reasonableness. Where the government seeks only data for which probable cause is established and limits officer discretion, geofence warrants are likely constitutional.

---

[242] *See id.* at 756.

This investigatory technique holds abundant potential for identifying unknown suspects who would otherwise evade identification and further investigation. The government has a great interest in finding those who commit serious crimes, especially when other methods have failed. This technique, like all others that invade a reasonable expectation of privacy, must adhere to the principles of the Fourth Amendment. With the right amount of care and specificity designed into the warrant application, it likely can.