Arizona Law Journal of Emerging Technologies

Volume 7 *Article 2*

2-2024

NAVIGATING THE TERRAIN OF GEOFENCE WARRANTS

Emily Brodner
University of Arizona James E. Rogers College of Law

2023-2024 https://azlawjet.com Vol. 7, Art. 2

Arizona Law Journal of Emerging Technologies

NAVIGATING THE TERRAIN OF GEOFENCE WARRANTS

Emily Brodner, J.D. Candidate 2024

Table of Contents

NAVIGATING THE TERRAIN OF GEOFENCE WARRANTS

Emily Brodner*

I. Abstract

This Note critically examines the legal intricacies surrounding geofence warrants in the context of the Fourth Amendment, delving into the evolving dynamics of privacy rights and law enforcement capabilities in the digital era. It provides an in-depth analysis of company policies, particularly those of major tech companies, and scrutinizes a range of federal opinions to assess the current legal stance on geofence warrants. The paper advocates for a judicious approach that balances individual privacy with the investigative needs of law enforcement, proposing a refined framework for the application of geofence warrants. This includes a recommendation for a two-step warrant process and clearly defined standards for probable cause, particularity, and overbreadth, aimed at aligning these warrants with constitutional principles and addressing the unique challenges posed by emerging technologies.

II. Introduction

Advancements in technology have ushered in a new era of Fourth Amendment challenges, particularly in how the law grapples with advanced data location tracking techniques used by law enforcement. Central to this Note is the use of geofence warrants. This novel investigative tool allows law enforcement to request location data from technology companies for devices within a specified area and time frame.[1]

Geofence warrants are used when the location of a crime is known but the suspects' identities are not.[2] Consequently, geofence warrants are unlike traditional Global Positioning System ("GPS") warrants, which routinely authorize law enforcement to locate a known suspect by tracking the individual's cell phone.[3] Geofence warrants thus reverse the approach by creating a digital boundary (the "geofence") around a location to collect location history data from all devices present during a specific time frame.[4]

Geofence warrants offer both benefits and concerns. The primary benefit of geofence warrants lies in their ability to solve crimes and catch criminals, primarily by generating

* J.D. Candidate, University of Arizona James E. Rogers College of Law, 2024. Thank you to Professors Derek Bambauer and Jane Bambauer for providing invaluable support and advice throughout the Note writing process. Thank you also to the entire Arizona Law Journal of Emerging Technologies staff for bringing this Note to publication. Finally, thank you to my family for their endless support and to my close friend, Isabella Cuevas, for always having open ears and a shoulder to lean on.

[1] United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022).

[2] *In re* Search of Info. That Is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 69 (D.D.C. 2021) [hereinafter *DC*].

[3] *Id.* at 68.

[4] *Id.* at 69–72.

leads and pinpointing suspects where conventional investigative methods fall short.[5] Additionally, they can exonerate the innocent by providing tangible evidence of a person's whereabouts during a crime.[6] However, accompanying these benefits are concerns because there is a lack of established legal precedent clearly delineating how these warrants comply with the Fourth Amendment.[7] The primary concern is that these warrants infringe upon privacy rights because location data is viewed as sensitive information.[8]

Since this is a novel investigative practice, the law regarding Fourth Amendment constitutionality is still developing.[9] By analyzing key case law, this paper aims to provide a comprehensive understanding of the current legal landscape while also addressing the evolving nature of privacy expectations in an increasingly connected world. The goal is to offer insights into how the law should adapt to ensure effective law enforcement practices while protecting individual privacy rights. First, this Note will describe big tech companies' policies for responding to a location data warrant request. Second, it will summarize the Fourth Amendment framework. Third, it discusses relevant federal geofence warrant decisions. Finally, it recommends a consistent framework that courts should follow.

III. Company Policies

The landscape of geofence warrant compliance varies among technology companies, any of which may become a target if they collect geolocation data.[10] While Apple, Lyft, Uber, Microsoft, and Yahoo have encountered geofence warrants, Google has been the primary target due to its extensive location data collection.[11] Google's approach to geofence warrants is transparent and complex, in stark contrast to the varied and less transparent policies other companies employ.

a. Google

Google received its first geofence warrant in 2016, and the frequency of such warrants has since escalated significantly, with a 1,500% increase from 2017 to 2018 and a 500% rise from 2018 to 2019.[12] By 2022, geofence warrants comprised more than 25 percent of all warrants Google received.[13]

Google amasses detailed location data on numerous users, storing it in a database known as "Sensorvault."[14] This data is primarily sourced from Google's "Location History"

[5] Mohit Rathi, *Rethinking Reverse Location Search Warrants*, 111 J. CRIM. L. & CRIMINOLOGY 805, 820 (2021).
[6] *Id.* at 822.
[7] *See id.* at 828–29.
[8] *Id.* at 807.
[9] *Id.* at 828–29.
[10] Matthew L. Brock, *"If You Build It, They Will Come": Reverse Location Searches, Data Collection, and the Fourth Amendment*, 57 U. RICH. L. REV. 649, 659–60 (2023).
[11] *See* Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2512–13 (2021); Zack Whittaker, *Google Moves to End Geofence Warrants, a Surveillance Problem it Largely Created*, TECHCRUNCH (Dec. 16, 2023, 9:30 AM), https://techcrunch.com/2023/12/16/google-geofence-warrants-law-enforcement-privacy/.
[12] United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022).
[13] *Id.*
[14] *Id.* at 907–08.

service, which captures a device's location approximately every two minutes, tracking it across every app and device linked to a user's account.[15] The data is impressively accurate, often within 20 meters, due to its collection from multiple sources like Bluetooth beacons, cellular towers, Wi-Fi networks, GPS, and IP addresses.[16] Location data is saved in Sensorvault once a user opts into "Location History," although it is notable that this feature is turned off by default.[17] However, even when a user chooses not to opt into Location History, Google can still track and store location data, as various services like Google Maps, web searches, and weather updates can transmit location information to Google.[18] This location data is traceable to a particular person because users must sign in to a Google account when using the cellphone or application.[19]

In response to privacy concerns over broad geofence warrants, Google, in 2018, began requiring all geofence warrants to include de-identification and narrowing measures.[20] This process involves multiple stages. First, law enforcement obtains a warrant directing Google to provide an anonymous list of users whose devices were within a specified geofence area and time frame.[21] The second stage involves authorities reviewing this data to narrow down devices of interest and, if necessary, compel Google to provide additional location data outside the original request's scope to help rule out irrelevant devices.[22] Finally, the third step permits authorities to request account-identifying information for users deemed relevant to the investigation.[23] Google prefers the number of users at this step to be fewer than in the second step, but it may approve requests even if they are not narrowed down.[24] As discussed in Part V, this multi-step process, or its variations, is now common in federal opinions reviewing geofence warrants.

In December 2023, Google announced a significant policy change: it would begin storing user Location History data on user devices rather than on Google's servers, making it impossible for Google to access.[25] This move ostensibly impedes Google's ability to respond to geofence warrants.[26] However, it is crucial to note that Google continues to collect and store substantial amounts of location data through other means and will likely still be able to respond to geofence warrants.[27] For instance, even if Location History is saved on the user's device, Google's privacy policy states: "Location History doesn't impact how location information is saved or used by Web & App Activity or other Google products, e.g., based on your IP address. You may still have other settings that save

[15] United States v. Rhine, 652 F. Supp. 3d 38, 67 (D.D.C. 2023).
[16] *Chatrie*, 590 F. Supp. 3d at 908, 936.
[17] *DC*, 579 F. Supp. 3d 62, 70 (D.D.C. 2021).
[18] *Id.* at 70 n.8.
[19] When creating a Google account, a user inputs identifying information such as their name, email address, and physical address. *Id.* at 79.
[20] *Chatrie*, 590 F. Supp. 3d at 914.
[21] *Id.* at 914–15.
[22] If a device was initially located within the geofence at step one, law enforcement could obtain all location data for that device over an extended time frame, whether inside or outside the geofence area. *Id.* at 916.
[23] This "includes the name and email address associated with the account." *Id.*
[24] *Id.*
[25] *See* Cyrus Farivar & Thomas Brewster, *Google Just Killed Warrants That Give Police Access to Location Data*, FORBES (Dec. 14, 2023, 5:43 PM), https://www.forbes.com/sites/cyrusfarivar/2023/12/14/google-just-killed-geofence-warrants-police-location-data/?sh=4c610dce2c86; Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, GOOGLE (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps/.
[26] Farivar & Brewster, *supra* note 25.
[27] *See* Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, AP NEWS (Aug. 13, 2018, 3:15 PM), https://apnews.com/article/828aefab64d4411bac257a07c1af0ecb.

location information."[28] Despite the policy change, Google is likely still equipped to respond to geofence warrants.

Consequently, this recent development in Google's policy does not diminish the relevance of geofence warrants. They continue to be a pivotal tool in law enforcement investigations, particularly given the vast location data Google collects and stores through other methods.

b. Other Tech Companies

The continued relevance of geofence warrants extends beyond Google to other technology companies. Despite Google's shift to storing location history data on user devices, which limits Google's compliance with geofence warrant requests, the policies of companies like Lyft, Uber, Microsoft, and Yahoo highlight the need for consistent standards in responding to such warrants. These companies continue to collect user location data but need more transparency in their warrant response policies. Establishing a uniform standard for responding to geofence warrants is vital for ensuring clarity and accountability. It allows users to understand how their location data is managed and shared with law enforcement, balancing the protection of user privacy with the effectiveness of criminal investigations.

Lyft has a clear policy regarding search warrants for GPS location information. Lyft requires these warrants to be supported by probable cause and is specific in its refusal to process overly broad or vague requests.[29] Lyft's policy mandates that search warrants must concisely identify the investigation or event that justifies the request by specifying the date, time, and locations involved.[30] Furthermore, the warrant must articulate what information is being sought, the reasons for its request, and its relevance to the investigation.[31] According to Lyft's transparency report from 2020, the company received 643 valid search warrants, complying with 534 of them.[32]

Uber's approach to disclosing GPS location data similarly necessitates a search warrant based on probable cause.[33] In Uber's view, a valid search warrant must specifically identify Uber Technologies Inc. as the entity to be searched and clearly state the person or property to be seized, such as user accounts, records, or content.[34] Uber's 2022 transparency report indicates that out of 1,653 search warrants received, data was provided for 1,122, affecting 3,003 users.[35]

---

[28] *Privacy & Terms*, GOOGLE, https://policies.google.com/technologies/location-data?hl=en-GBhttps://policies.google.com/technologies/location-data?hl=en-GB (last visited Dec. 22, 2023).
[29] *Lyft's Law Enforcement Support*, LYFT, https://help.lyft.com/hc/en-us/all/articles/115012925607-Lyft-s-law-enforcement-support (last visited Dec. 21, 2023).
[30] *Id.*
[31] *Id.*
[32] Lyft's report does not categorize geofence warrant requests separately. *Id.*
[33] *Guidelines for United States Law Enforcement*, UBER, https://www.uber.com/legal/en/document/?uclick_id=649e0c96-a364-474c-97f2-f5c0616844fc&country=united-states&lang=en&name=guidelines-for-law-enforcement#kix.1lhvmrnrzlqk (last modified Dec. 21, 2023).
[34] *Id.*
[35] Like Lyft, Uber does not separately categorize requests about geofence warrants. *Transparency Report*, UBER (June 9, 2023), https://www.uber.com/us/en/about/reports/transparency/law-enforcement/?uclick_id=649e0c96-a364-474c-97f2-f5c0616844fc.

Microsoft obtains location data from a variety of sources[36] and requires a search warrant "to obtain content or location information (over an extended period) . . . ."[37] Additionally, it states that "requests should be targeted at a specific account, identifier or device . . . should only be approved when they are supported by specific evidence that demonstrates criminal conduct and . . . the [required] data [is connected to] an investigation of a serious criminal offense."[38]

Lastly, Yahoo, which collects location data from various sources, adheres to a policy allowing it to access, preserve, and disclose information in connection with legal processes and requests.[39] In the first half of 2022, Yahoo received 1,666 search warrant requests, disclosing data in response to 1,397 and affecting 2,597 accounts.[40]

IV. The Fourth Amendment

The Fourth Amendment states:

> 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.[41]

The overall goal of this provision is to protect an individual's right to privacy from unreasonable government intrusion.[42] It does so through two clauses: the reasonableness clause and the warrant clause. The reasonableness clause assesses whether a government action constitutes an unreasonable search or seizure by infringing upon an individual's protected privacy interest.[43] The warrant clause requires the government to obtain a warrant backed by probable cause for any search or seizure, barring a limited set of exigent circumstances.[44]

---

[36] *Location Sharing and Your Privacy*, MICROSOFT, https://support.microsoft.com/en-au/topic/location-sharing-and-your-privacy-337b635f-2e61-4c06-b51a-96d004582f47 (last visited Dec. 23, 2023).
[37] The definition of "extended period" is unknown. *Six Principles for International Agreements Governing Law-Enforcement Access to Data*, MICROSOFT, https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/09/SIX-PRINCIPLES-for-Law-enforcement-access-to-data.pdf (last visited Dec. 21, 2023).
[38] *Id.*
[39] *See Welcome to the Yahoo Privacy Policy*, YAHOO!, https://legal.yahoo.com/us/en/yahoo/privacy/index.html (last updated July 2023).
[40] In the first half of 2022, Yahoo received 1,666 search warrant requests, disclosing data in response to 1,397 of these, affecting 2,597 accounts. *Law Enforcement Data Requests*, YAHOO!, https://www.yahooinc.com/transparency/reports/government-data-requests/country/united-states/jan-jun-2022/index.html (last visited Jan. 29, 2024); *Frequently Asked Questions*, YAHOO!, https://www.yahooinc.com/transparency/about/faq-glossary.html (last visited Dec 22, 2023).
[41] U.S. CONST. amend. IV. (emphasis added).
[42] Wex Definitions Team, *Fourth Amendment*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/fourth_amendment#:~:text=Reasonableness%20Requirement,of%20a%20search%20or%20seizure (last updated May 2023).
[43] *Id.*
[44] *Id.*

a. An Unreasonable Search

Central to the Fourth Amendment is that it "protects people, not places, . . ." with the touchstone being reasonableness.[45] A search is deemed reasonable or not by weighing "the degree to which it intrudes upon an individual's privacy . . ." interest and the degree to which the search "is needed to promote legitimate governmental interests."[46] Government action qualifies as a search when it intrudes into an area where a person has a reasonable expectation of privacy,[47] a standard originally established by Justice Harlan's two-prong reasonable expectation of privacy test in *Katz v. United States*.[48] Under this test, a search occurs when (1) an individual exhibits an actual, subjective expectation of privacy and (2) this expectation is one society is prepared to recognize as reasonable.[49] Intrusion into this realm generally constitutes a search requiring a warrant.[50]

The protection of privacy interests in location data maintained by a third party is situated at the convergence of two distinct case law streams: those addressing "a person's expectation of privacy in his physical location and movements" and those addressing "what a person keeps to himself and what he shares with others."[51]

i. Expectations of Privacy in Physical Location and Movements

The concept of privacy in one's physical movements evolved through three seminal cases: *United States v. Knotts*,[52] *United States v. Jones*,[53] and *Carpenter v. United States*.[54] In *Knotts*, the Court found no Fourth Amendment violation in the government using a beeper to track a car for a few hours as it traveled on public roads.[55] This decision rested on the notion that the defendant had "no reasonable expectation of privacy in his movements from one place to another" while traveling on public roads because his movements were "voluntarily conveyed to anyone who wanted to look . . . ."[56] However, *Knotts* left open the possibility that more pervasive surveillance could trigger Fourth Amendment concerns.[57]

Nevertheless, in *Jones* and *Carpenter*, the Court acknowledged such privacy concerns associated with long-term GPS monitoring and cell site location information ("CSLI"),

[45] *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (U.S. 2018) (quoting Smith v. Maryland, 442 U.S. 735, 739 (1979)); *DC*, 579 F. Supp. 3d 62, 76 (D.D.C. 2021).
[46] *DC*, 579 F. Supp. 3d at 76 (quoting United States v. Knights, 534 U.S. 112, 112–13 (2001)).
[47] *Carpenter*, 138 S. Ct. at 2213. The trespass theory is another theory to determine whether a search occurred. It is inapplicable to this Note. *See id.*
[48] *Id.*; Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).
[49] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
[50] *Carpenter*, 138 S. Ct. at 2213. For example, in *Katz v. United States*, the Court held that a Fourth Amendment search occurred when the government attached a device to an enclosed telephone booth to eavesdrop on the defendant's conversation without his consent or knowledge. The Court reasoned that, despite the telephone booth's public nature, a warrant was required because the defendant could assume his conversation "[would] not be broadcast to the world." 389 U.S. at 348, 352.
[51] *Carpenter*, 138 S. Ct at 2214–16.
[52] 460 U.S. 276 (1983).
[53] 565 U.S. 400 (2012).
[54] 138 S. Ct. 2206 (U.S. 2018).
[55] *Knotts*, 460 U.S. at 281–82, 285.
[56] *Id.* at 281–82.
[57] *Id.* at 283–84.

recognizing a reasonable expectation of privacy in the whole of an individual's physical movements.[58] In *Carpenter,* the Court held that accessing seven days of CSLI constituted a search because it provided an intimate window into a person's life by revealing his "familial, political, professional, religious, and sexual associations" through his movements.[59] Notably, the Court explicitly stated that this holding only relates to historical CSLI and no other matters not before them—such as geofence location data.[60]

In sum, the distinction between these cases lies in the duration and invasiveness of the tracking. While short-term observation in public is permissible without a warrant, long-term tracking that reconstructs an individual's movements is not.

ii. What a Person Keeps to Himself and What He Shares with Others

The second line of cases concerns information shared with third parties. Under the third-party doctrine, an individual has "no legitimate expectation of privacy in information he voluntarily turns over to third parties,"[61] "even if the information is revealed on the assumption that it will be used only for a limited purpose . . . ."[62] Therefore, the government can generally obtain this type of information from a third party without triggering Fourth Amendment protections.[63] The Supreme Court established the third-party doctrine in *United States v. Miller* and *Smith v. Maryland*, where the Court held that information voluntarily exposed to third parties do not warrant Fourth Amendment protections.[64]

However, the Supreme Court limited this principle in *Carpenter v. United States*, recognizing individuals can have a privacy interest in CSLI held by wireless carriers because that information is not truly shared voluntarily.[65] The Court distinguished *Carpenter* from earlier cases, noting that (1) carrying a cell phone is "indispensable to participation in modern society," (2) apart from disconnecting from the network, there is no way to truly opt out of creating a trail of location data because (3) the records are created "by dint of its operation, without any affirmative act on the part of the user beyond

[58] *See Jones*, 565 U.S. at 415, 430 (Alito, J., concurring), (Sotomayor, J., concurring) (indicating that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy" whether or not those movements are disclosed to the general public); *Carpenter*, 138 S. Ct. at 2217, 2220 (citing United States v. Jones, 565 U.S. 400, 430 (2012)) (Alito, J., concurring) (recognizing that "individuals have a reasonable expectation of privacy in the whole of their physical movements," even when traveling on public streets).
[59] *Id.* at 2217 n.3.
[60] *See id.* at 2220. Thus, the holding suggests "that less than seven days of location information may not require a warrant." *Id.* at 2234 (Kennedy, J., dissenting).
[61] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
[62] United States v. Miller, 425 U.S. 435, 443 (1976).
[63] *Carpenter*, 138 S. Ct. at 2216.
[64] *Miller*, 425 U.S. at 442–43 (holding that the defendant did not have a reasonable expectation of privacy in checks voluntarily conveyed to banks because they were exposed to employees in the ordinary course of business); *see also Smith*, 442 U.S. at 743–44 (holding that using a pen register to record dialed phone numbers does not constitute a search, as individuals do not have an expectation of privacy society recognizes as reasonable in dialed phone numbers given these are automatically conveyed to and used by the phone company for various purposes, a fact commonly understood by society).
[65] *Carpenter*, 138 S. Ct. at 2220.

powering up."[66] After the *Carpenter* decision, the question for a defendant seeking to exclude geofence evidence is whether opting into location services is truly voluntary.[67]

b. Warrant Requirement

Under the Fourth Amendment, a warrant must fulfill three elements: (1) it must be supported by probable cause, (2) it must be sufficiently particular, and (3) it must be issued by a neutral, disinterested magistrate.[68]

For search warrants of property, the first element—probable cause—requires satisfying two components.[69] First, there must be a fair probability that (i) a crime was committed, and (ii) contraband or evidence of that crime will be found at the place to be searched.[70] Second, sufficient evidence must demonstrate a nexus between the criminal activity and the location to be searched.[71]

The second element—sufficient particularity—requires a warrant to particularly describe the place to be searched and the person or things to be seized, thereby limiting the executing officer's discretion and defining the search's scope.[72] For places to be searched, "it is enough if the description is such that the officer with a search warrant can, with reasonable effort ascertain and identify the place intended."[73] For the things to be seized, particularity depends on "what is realistic or possible for the investigation at hand."[74] Absolute precision is not required—"generic descriptions of the items to be seized are sufficient so long as they particularize the types of items to be seized."[75] Moreover, the warrant must avoid being overbroad; a requirement distinct but related to particularity.[76] The overbreadth requirement ensures the items listed for seizure are not "broader than the probable cause on which it is based."[77]

V. Survey of Geofence Warrant Federal Opinions

At the time of this writing, there is a scarcity of case law addressing geofence warrants. There has been a total of twelve federal opinions specifically addressing geofence warrants.[78] As elaborated below, there is no court opinion determining whether one can

---

[66] *Id.*
[67] Orin S. Kerr, *The Fourth Amendment and Geofence Warrants: A Critical Look at* United States v. Chatrie, REASON (March 11, 2022, 4:38 PM), https://reason.com/volokh/2022/03/11/the-fourth-amendment-and-geofence-warrants-a-critical-look-at-united-states-v-chatrie/.
[68] Dalia v. United States, 441 U.S. 238, 255 (1979).
[69] *See In re* Search of Information Stored at Premises Controlled by Google, No. 2:22-mj-01325, 2023 WL 2236493, at *7 (S.D. Tex. Feb. 14, 2023) [hereinafter *Texas*]; *DC*, 579 F. Supp. 3d 62, 75 (D.D.C. 2021).
[70] *Texas*, 2023 WL 2236493, at *7.
[71] *See DC*, 579 F. Supp. 3d 62, 75 (D.D.C. 2021).
[72] *Texas*, 2023 WL 2236493, at *10.
[73] *Id.* (quoting Steele v. United States, 267 U.S. 498, 503 (1925)) (internal quotation marks omitted).
[74] *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 357 (N.D. Ill. 2020) (citing Archer v. Chisholm, 870 F.3d 603, 616 (7th Cir. 2017)) [hereinafter *Arson Investigation*].
[75] *Id.* (citing *Archer*, 870 F.3d at 616).
[76] *Texas*, 2023 WL 2236493, at *11.
[77] United States v. Chatrie, 590 F. Supp. 3d 901, 928 (E.D. Va. 2022) (quoting United States v. Hurwitz, 459 F.3d 463, 473 (4th Cir. 2006)). A warrant is overbroad if it encompasses items beyond the scope of the evidence establishing probable cause. *Id.*
[78] *See generally* United States v. Wright, No. CR419-149, 2023 WL 6566521 (S.D. Ga. May 25, 2023), *aff'd in part*, No. 4:19-cr-149, 2023 WL 5804161 (S.D. Ga. Sept. 7, 2023) (issued geofence warrant);

have a reasonable expectation of privacy in their location data, nor is there a consistent analysis for determining the validity of a geofence warrant. This Note will discuss the different approaches in six opinions chronologically.

a. A Geofence Warrant Application is Approved for an Arson Investigation

A magistrate judge for the Northern District of Illinois approved a geofence warrant application for location data related to a string of arsons in Chicago.[79] The court focused solely on the warrant's validity, sidestepping whether individuals have a reasonable expectation of privacy in their location data.[80] Unlike Google's multi-step process, this warrant application involved a two-step process for obtaining Google's location data.[81] In the first step, Google would provide anonymized data for devices within the government's defined geofence area and time frames.[82] In the second step, the government, at its discretion, would identify the specific devices for de-anonymization.[83]

First, the warrant application established there was probable cause that (a) "crimes of arson and conspiracy to commit arson occurred," and (b) "evidence of the crime [would] be located at Google because location data on cell phones at the scene of the arson, as well as the surrounding streets, [could] provide evidence on the identity of the perpetrators and witnesses to the crime."[84] Despite no direct evidence linking suspects to cell phones or Google during the arsons, the court found probable cause based on location data providing evidence of perpetrators or witnesses because the agent's affidavit described the multiple arsons, the evidence linking them together, and explained that based on the agent's experience, co-conspirators commonly used cell phones to communicate during crimes.[85] Moreover, the court noted, "it is rare to search an individual in the modern age during the commission of a crime and not find a cell phone on the person."[86]

Regarding particularity and overbreadth, the court found the geofence warrant complied with the Fourth Amendment's requirements by being narrowly tailored in time and

United States v. Carpenter, No. 8:21-cr-309-VCM-MRM, 2023 WL 3352249 (M.D. Fla. Feb. 28, 2023) (issued geofence warrant); *Texas*, 2023 WL 2236493 (geofence warrant application); United States v. Smith, No. 3:21-cr-107-SA, 2023 WL 1930747 (N.D. Miss. Feb. 10, 2023) (issued geofence warrant); United States v. Rhine, 652 F. Supp. 3d 38 (D.D.C. 2023) (issued geofence warrant); *Chatrie*, 590 F. Supp. 3d 901 (issued geofence warrant); *DC*, 579 F. Supp. 3d 62 (D.D.C. 2021) (geofence warrant application); United States v. Davis, No. 2:21-cr-101-MHT-JTA, 2022 WL 3009240 (M.D. Ala. July 1, 2022) (issued geofence warrant); *In re* Search of Info. That Is Stored at the Premises Controlled by Google, LLC, 542 F. Supp. 3d 1153 (D. Kan. 2021) [hereinafter *Kansas*] (geofence warrant application); *Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020) (geofence warrant application); *In re* Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730 (N.D. Ill. 2020) (geofence warrant application); *In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020) (geofence warrant application).

[79] *Arson Investigation*, 497 F. Supp. 3d at 349.

[80] *Id.* at 360.

[81] *Id.* at 353.

[82] *Id.*

[83] *Id.*

[84] *Id.* at 355. Specifically, the video surveillance and investigation by the Chicago Fire Department indicated that the deliberate burning of multiple cars constituted a violation of federal laws against malicious destruction of property and conspiracy. *Id.* at 354–55.

[85] The agent's experience also detailed Google's methods of collecting location data. *Id.* at 354–57.

[86] *Id.* at 356.

location.[87] The warrant was sufficiently particularized because the time frames were limited to 15 to 30 minutes at the approximate time of the arsons, and the target locations were limited to the arson sites and streets leading to and from those sites.[88]

Moreover, the court determined that based on the warrant's construction and the agents' prior investigations, the warrant was limited in scope and "would not result in the collection of a broad sweep of data from uninvolved individuals for which there is no probable cause."[89] The warrant was constructed to narrowly tailor the locations and times to likely capture only location data of those connected to the arsons.[90] This was supported by the agents' investigations, which included analyzing camera footage to monitor pedestrian activity—showing little activity—and assessing the occupancy status of nearby buildings during the relevant time frames, which were closed during the geofence time frames.[91] However, the court found the two-step process "[did] not ameliorate any constitutional concerns" or minimize overbreadth concerns because the government retained the discretion of obtaining any deanonymized data it so chose in the second step.[92] Yet, the court granted the warrant application because "the government . . . established probable cause to seize all location and subscriber data within the geofence locations identified."[93]

b. Kansas Denies a Geofence Warrant Application

A magistrate judge for the District of Kansas denied a geofence warrant application after finding it lacked probable cause and particularity.[94] While the application established probable cause that a crime occurred, it did not establish any probability that "the identity of the perpetrator or witnesses would be encompassed within the search."[95] The application lacked evidence suggesting the suspect or a witness possessed a smartphone, and, despite the court assuming widespread cell phone usage, the application failed to demonstrate a reasonable likelihood that any relevant individual was using a device connected to Google's location-tracking technology.[96]

Additionally, the application lacked sufficient particularity because it failed to narrowly define the place to be searched by time and location, and thus, was overbroad.[97] First, the one-hour time frame needed to be justified.[98] The requested one-hour window not only surpassed the time frame in other geofence warrant cases, but also appeared poorly aligned with the specific criminal activity depicted in the application.[99] Surveillance footage showed the suspect's presence at three distinct times, yet the geofence's temporal scope strangely omitted the first sighting and strangely encompassed the entire period

[87] *Id.* at 358.
[88] *Id.* at 357.
[89] *Id.* at 358–59.
[90] *Id.*
[91] *Id.*
[92] *Id.* at 362.
[93] *Id.*
[94] *Kansas*, 542 F. Supp. 3d 1153, 1154 (D. Kan. 2021). This opinion did not discuss any multi-step process that may have been detailed in the warrant application.
[95] *Id.* at 1157.
[96] *Id.*
[97] *Id.* at 1158.
[98] *Id.*
[99] *Id.*

between the second and third sightings.[100] The application offered no explanation for these curious gaps, leaving the court unable to discern the rationale behind the chosen time frame.[101]

Second, the proposed geofence area was not limited in a way to exclude data of individuals who had nothing to do with the crime because it encompassed two public streets and a business.[102] In contrast with the *Arson Investigation*[103] application, this application failed to explain the extent to which the geofence would capture uninvolved individuals from the streets and businesses.[104]

Nevertheless, the court asserted that the government could fix this geofence application by either redrawing the parameters of the request or explaining the extent to which uninvolved individuals' data would be collected, along with its reasoning behind the location and time frame requests.[105]

c. The District of Columbia Approved a Geofence Warrant Application

A magistrate judge for the District of Columbia granted a geofence warrant application that implemented a different two-step process to obtain identified location data.[106] In step one, Google would provide an anonymized list of devices within the geofence during specified times.[107] In step two, the government would *return to the court* and justify the need to deanonymize specific devices based on its review of the anonymized information provided by step one and other evidence in the case.[108] In step two, if the justification aligned with the established probable cause, the court would direct Google to disclose the de-identified device information to the government.[109] Although the court did not definitively decide whether individuals have a reasonable expectation of privacy in their location data, they noted that while step one likely did not implicate privacy concerns, step two may trigger Fourth Amendment protection.[110]

Based on video surveillance showing the criminal activity and the suspects using their phones, the court found probable cause to believe that a crime was committed, and evidence of that crime—the suspects' identities—would be found on Google's servers.[111] While the government did not specifically allege the cell phones were transmitting to

[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] In the *Arson Investigation*, the agents' investigations found that few pedestrians were out, and nearby businesses were closed during the time frame. *Supra* Part V(A).
[104] *Kansas*, 542 F. Supp. 3d at 1158.
[105] *Id.* at 1158–59.
[106] *DC*, 579 F. Supp. 3d 62, 73–74, 91 (D.D.C. 2021).
[107] *Id.* at 88.
[108] *Id.*
[109] *Id.* at 89.
[110] *Id.* at 89 n.26.
[111] In a brief summary, the court stated that "because there [was] a 'fair probability' that (i) the suspects were inside the geofence, (ii) were using their cell phones inside the geofence, (iii) those phones communicated location information to Google, and (iv) Google [could] trace that information back to a particular device, accountholder, and/or subscriber, there [was] probable cause that the search [would] produce evidence useful to the government's investigation of the criminal activity in question." *Id.* at 77, 79.

Google, the court however noted "it would be the 'relatively rare' case [for] a cell phone [to] not transmit location information to Google" and only a fair probability of such was required.[112]

Further, the court ruled that the warrant was sufficiently particular when it described the data for law enforcement to seize in categories of their designated crimes and limited their ability to search the place in time and location.[113] Additionally, although the time frame spanned 185 minutes over nearly six months, it was limited in scope by targeting the specific moments when video observed the suspects committing the crime.[114] Moreover, the geofence location was limited to a portion of the business center—the place of the offense—and the adjoining parking lot, such that no other structures were included, including the rest of the building shared with other businesses.[115]

The court held that the warrant was not overly broad because the time frame and location closely tracked the probable cause presented—it was limited to the exact time of the crime and locations the suspects were known to be present or associated with—and subsequent investigation minimized the possibility of collecting uninvolved individual's data.[116] The court defined the two-step process as "subsequent investigation" that ameliorated overbreadth concerns because it served as a "court-supervised filter" that ensured there was particularized probable cause for each device in which law enforcement sought identifying information.[117]

Lastly, the court emphasized that the possibility of collecting uninvolved third-party location data was not fatal to the warrant application's constitutionality because "constitutionally permissible searches may infringe on the privacy interests of third persons . . . ."[118] It highlighted that the public interest in implementing the law outweighed "the privacy interests which could be indirectly impacted by a legal search backed by probable cause."[119] Finally, in concluding that it would not be unconstitutional to collect uninvolved data when the property search warrant standard had been met, the court stated that "particularity turns on what is realistic or possible in *this* investigation," and in this case, it was not possible to have constructed the geofence in a way to exclude everyone besides the suspects.[120]

[112] The court further explained that "[r]oughly three-quarters of all phones worldwide contain Google's [operating system], and even those phones without Google's [operating system] nonetheless have access to popular Google applications, the use of which can cause location information to be transmitted to Google." *Id.* at 78. Thus, "even if only a third of Google [operating system] users opt-in to the 'Location History' service, that figure—which numbers in the 'numerous tens of millions' of users—likely underestimates the volume of location information Google possesses, since (a) the government aver[red] that Google collects location data even for users who have requested that such data not be gathered and (b) Google can collect location information from non-Google devices (e.g., iPhones) if those device users utilize Google accounts on those devices." *Id.* at 79.
[113] *Id.* at 79–80.
[114] *Id.* at 81.
[115] *Id.* at 82.
[116] *Id.* at 80–81, 90.
[117] *Id.* at 89–90.
[118] *Id.* at 82.
[119] *Id.* at 83–84.
[120] *Id.* at 85 (quoting Archer v. Chisholm, 870 F.3d 603, 616 (7th Cir. 2017)).

d. *United States v. Chatrie* Found a Geofence Warrant Unconstitutional

In the first federal case analyzing an issued geofence warrant, a district court judge for the Eastern District of Virginia found the geofence warrant unconstitutional because it lacked particularized probable cause for *each* and *every* device within the geofence.[121] Despite the court finding this geofence warrant unconstitutional, the good faith exception shielded the evidence from suppression.[122] In this case, the geofence warrant implemented Google's exact three-step framework for obtaining location history data, seeking data for a one hour time frame across a 150 meter radius centered around the crime scene.[123]

Because the good-faith exception applied, the court declined to decide whether the defendant had standing—i.e., a reasonable expectation of privacy in his location data.[124] However, the court noted it was unlikely the third-party doctrine applied, reasoning that the defendant could not voluntarily disclose location data because Google's warnings about location data collection were limited and vague when the defendant opted into Location History services.[125]

Regarding particularized probable cause, the court asserted the warrant "must establish probable cause that is particularized with respect to the person to be searched or seized."[126] Based on this rule, it disagreed with the government that the warrant established "probable cause to obtain *all* information (Steps 1, 2, and 3) from *all* users within the geofence without any narrowing measures."[127] The court explained the warrant lacked "any suggestion that all—or even a substantial number of—the individuals searched had participated in or witnessed the crime," and the captured location data included individuals "who may not have been remotely close enough" to be a suspect or witness.[128]

Thus, although the government sufficiently asserted the suspect was using his cell phone within the geofence area, thereby creating a fair probability that the warrant would generate the *suspect's* location data, the court found that—without more—this did not

[121] United States v. Chatrie, 590 F. Supp. 3d 901, 929 (E.D. Va. 2022).
[122] *Id.* at 937. The good faith exception provides that "evidence obtained during the execution of a warrant later determined to be deficient is nonetheless admissible if the executing officer's reliance on the warrant was objectively reasonable and made in good faith." United States v. Massi, 761 F.3d 512, 525 (5th Cit. 2014) (quoting United States v. Woerner, 709 F.3d 527, 533 (5th Cir. 2013)). The exclusionary rule applies only if the "affidavit of probable cause is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable" United States v. Rhine, 652 F. Supp. 3d 38, 89, (D.D.C. 2023) (quoting United States v. Griffith, 867 F.3d 1265, 1278 (D.C. Cir. 2017)) (internal quotation marks omitted). In *Chatrie*, the court reasoned that at the time of the case, no court had ruled on the legality of geofence warrants, making the officer's reliance reasonable. *Chatrie*, 590 F. Supp. 3d at 937–38.
[123] (1) Google would produce an anonymized list; (2) the government could request Google to provide additional location data outside the original request's scope; (3) the government would identify, at its discretion, a subset for which it wanted identifying information. *Id.* at 918–21, 935–36.
[124] Specifically, the court stated that standing is best left to the legislature because geofence warrants do not fit within existing reasonable expectations of privacy precedent. *Id.* at 925–26.
[125] *Id.* at 935–36.
[126] *Id.* at 929 (quoting Maryland v. Pringle, 540 U.S. 366, 366 (2003)) (internal quotation marks omitted).
[127] *Id.* (emphasis in original).
[128] *Id.* at 929–30.

justify the expansive geofence warrant.[129] Moreover, unlike in *DC*, the warrant's three-step process did not resolve its lack of particularity, giving officers too much discretion without adequate judicial oversight.[130] Notably, the warrant needed more specific language to identify which accounts officers would objectively scrutinize further, and it needed to set clear criteria or limits for obtaining identifying information.[131] This landmark case is now poised to set precedent at the appellate level, as *United States v. Chatrie* will be the first geofence warrant case to be scrutinized by any federal court of appeals, marking a significant step in the judicial examination of digital privacy rights.[132]

e. *United States v. Rhine* Found a Geofence Warrant Constitutional

In a United States Capitol riot case, a district court judge for the District of Columbia upheld a geofence warrant, finding it constitutionally valid on both probable cause and particularity grounds.[133] Moreover, the good faith exception would have applied even if the warrant lacked particularized probable cause.[134]

In this case, a different multi-step process was implemented.[135] At step one, the government received a primary list of devices within the geofence during the relevant time frame and two control lists of devices within the geofence, but only at times outside the time frame.[136] At step two, the government reviewed and eliminated devices appearing on both lists.[137] Finally, at step three, the government requested identified data for the remaining devices within the geofence location.[138]

To begin, like all prior cases, the court declined to decide whether the defendant had a reasonable expectation of privacy in his location data and focused solely on the constitutionality of the geofence warrant.[139] The court found probable cause to believe that a crime had been committed because merely entering the Capitol building during the designated time frame constituted a crime, considering that the Capitol was closed for the Electoral College vote counting.[140] Furthermore, corroborating evidence in the form of surveillance footage, news coverage, photographs, and videos taken by the suspects while inside the Capitol showed the suspects were possessing a cell phone.[141] The court concluded "there was much more than a 'fair probability' that the suspects were within the geofence area and were carrying and using smartphones while there, such that their

[129] *Id.*
[130] *See DC*, 579 F. Supp. 3d 62, 87–91 (D.D.C. 2021); *Id.* at 934.
[131] The warrant did not limit the number of devices from which identifying information could be requested. *Id.*
[132] The Court of Appeals for the Fourth Circuit will provide the opinion. Philip Glaser, *Geofence Warrants: Strict in Theory. Fatal in Fact?*, UNIV. OF BALT. L. REV. (Oct. 22, 2023), https://ubaltlawreview.com/2023/10/22/geofence-warrants-strict-in-theory-fatal-in-fact/.
[133] United States v. Rhine, 652 F. Supp. 3d 38, 89–90 (D.D.C. 2023).
[134] *Id.*
[135] *Id.* at 68–69.
[136] *Id.* at 83–84.
[137] The court noted that "the purpose of using control lists from outside the step one timeframe was to narrow the universe of devices to ensure that the supplemental affidavit seeking deanonymization established particularized probable cause." *Id.* at 84.
[138] *Id.* at 84–85.
[139] *Id.* at 82.
[140] *Id.* at 85.
[141] *Id.*

devices' [location history] would provide evidence of a crime."[142] The court noted that these facts, combined with the large number of suspects, make the scope of probable cause "unusually broad."[143]

The court found the geofence warrant was sufficiently particular because it was temporally and geographically particular by requesting data "between 2:00 pm and 6:30 pm on January 6, 2021 for individuals in a target area slightly larger than but roughly tracing the contours of the Capitol building itself . . . ."[144] Furthermore, the warrant narrowly described the things to be seized by categorizing the location data and imposing limitations on what data could be seized.[145]

Lastly, the court ruled the geofence warrant was not overly broad.[146] First, the warrant's geographic area closely matched the parameters of the Capitol building and excluded adjacent plazas, grounds, businesses, and residences.[147] Second, the four-and-a-half-hour time frame, exceeding most geofence warrants, was justified by its alignment with official timelines indicating the time the breach began to the time the building was secure.[148] Finally, the warrant's three-step data deanonymization process effectively narrowed down the data request, reducing the number of devices for deanonymized information by 73%.[149]

f. Texas Approves a Geofence Warrant Application

A magistrate judge for the Southern District of Texas approved a geofence warrant application concerning an investigation of identity theft and unauthorized withdrawals from multiple bank accounts.[150] The application proposed a two-step process similar to the one in *DC*: law enforcement initially sought a geofence warrant for anonymized data supported by particularized probable cause.[151] After analyzing this data to identify potential suspects, law enforcement would *return to the court* and request a subsequent warrant for specific, deanonymized location data.[152]

As with the previous cases, the court declined to decide whether there was a reasonable expectation of privacy in location data held by a third party but hinted there likely is.[153] The court distinguished this case from *Carpenter v. United States* in a few ways.[154] First, the court found it important that the data produced from step one is anonymized, stating

[142] *Id.*
[143] *Id.*
[144] *Id.* at 68, 86–88.
[145] The court noted that Section II in the warrant set out the categories of items to be seized, and other sections limited Section II to "information described in Section I that constitutes evidence of listed offenses." Moreover, Section I only authorized the search of location data and account information for devices with responsive data—i.e., devices with one location point within the Capitol building. *Id.* at 88–89.
[146] *Id.* at 88.
[147] *Id.* at 86–87.
[148] *Id.* at 88.
[149] *Id.* at 83–86.
[150] There were 44 unauthorized withdrawals occurring at the same location, with most recorded on video. *Texas*, No. 2:22-mj-01325, 2023 WL 2236493, at *1 (S.D. Tex. Feb. 14, 2023).
[151] *See DC*, 579 F. Supp. 3d 62, 87–90 (D.D.C. 2021); *Id.* at *6.
[152] *Texas*, 2023 WL 2236493, at *6.
[153] *Id.* at *8.
[154] The court even stated the case before it was "a far cry from *Carpenter*." *Id.*

"a person does not have a reasonable expectation of privacy over information that cannot be connected to her."[155] Second, the time period involved was much more brief—105 minutes over 21 days—than the time period in *Carpenter*.[156] The court explained society has recognized short-term monitoring of public movements as reasonable, and in the instant case, the "anonymized geofence information sought . . . [was] plainly short-term in nature, covering a maximum of 17 minutes on any one occasion."[157]

Looking at probable cause, the court determined there was sufficient probable cause to collect anonymized data from the entire geofence area.[158] First, there was probable cause to believe a crime occurred when unauthorized withdrawals were made with the account holder's social security number.[159] Next, the court reasoned there was probable cause to believe evidence of the crime would be found on Google's servers for three reasons: (1) there was surveillance video showing a suspect with a phone, (2) co-conspirators often carry cell phones to communicate with each other, and (3) cell phones "are ubiquitous in people's daily lives."[160]

Looking at particularity, the court found it sufficient when the application identified Google servers as the specific location where the evidence would be found, described the geographic area with latitude and longitude information to six decimal places worth of specificity, specified 105 minutes as the geofence time frame, and asserted the information to be seized as "Location History information stored on Google's servers."[161]

Regarding overbreadth, the court stated, "[t]o determine whether the warrant application is overbroad, the Court assesses whether the proposed authorization to seize all of the requested Google Location History information for all devices within the polygon during the stated time periods is supported by probable cause."[162] Based on this rule, the warrant was not overbroad for two reasons: the time frame showed a close nexus to the criminal activity when it coincided with the unauthorized withdrawals, and the geofence area was narrow enough to likely capture only evidence of the crime because it was limited to the area of the crime and its access points.[163] Further, similar to the narrowing measure in *Rhine*, the application requested data stretching a few minutes after each unauthorized withdrawal to eliminate uninvolved devices from step two consideration.[164]

Finally, the court found the two-step process was an additional protection against overbreadth.[165] Obtaining only anonymized data in step one minimized privacy intrusion

---

[155] *Id.* (quoting Sanchez v. Los Angeles Dept. of Transp., No. CV205044DMGAFMX, 2021 WL 1220690, at *3 (C.D. Cal. Feb 23, 2021)). "No one's whereabouts [would] be learned . . . and no one's movements [would] be tracked or catalogued. No one's 'familial, political, professional, religious, or sexual associations' [would] be divined from the information disclosed pursuant to the warrant." *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).
[156] *Id.* at *7–8. *Carpenter* involved 127 days' worth of CSLI. *Id.* at *7.
[157] *Id.* at *8.
[158] *Id.* at *13.
[159] *Id.* at *9.
[160] *Id.*
[161] The court stated that merely describing the place to be searched as the servers owned by Google satisfies the particularity requirement because law enforcement cannot be reasonably expected to know which Google servers, in a specific location, would contain evidence of the crime. *Id.* at *10–11.
[162] *Id.* at *11.
[163] *Id.* at *11–13.
[164] *Id.* at *12–13.
[165] *Id.* at *13.

for potentially irrelevant individuals, and identifying specific devices for further scrutiny in step two required returning to the court to justify the specific devices they were interested in supported by probable cause.[166] Although the step one disclosure may have included uninvolved third parties, this did not render the warrant overbroad when weighed against the interest of identifying the suspects because the data was anonymized.[167]

VI. Recommendations

Geofence warrants have created multiple problems that test the limits of the Fourth Amendment. First, it is unclear whether an individual has a reasonable expectation of privacy in their location data held by companies. Moreover, scholars, courts, and legislators cannot get on the same page regarding the geofence warrant standard. This is problematic because law enforcement has little guidance on the use of geofence warrants. In light of this lack of guidance, all five federal cases considering the constitutionality of issued geofence warrants noted that the good faith exception shields the evidence from suppression.[168] With proper guidelines, geofence warrants will create benefits that outweigh privacy intrusions—enhancing public safety while reinforcing the criminal justice system by preventing criminals from getting off on crimes.[169]

a. Courts Should Adopt a Two-Step Process with Judicial Oversight

Courts should adopt the two-step process used by the District Court for the District of Columbia and the District Court for the Southern District of Texas.[170] In the first step, law enforcement would head to the courts and apply for a geofence warrant requesting *anonymous* location data supported by particularized probable cause.[171] If the court determines the application shows particularized probable cause—limited in time, location, and scope—the company will then furnish law enforcement with anonymous user location data for the entire geofence area during the specified time frame.[172] In the second step, after analyzing this data and identifying relevant devices, law enforcement must *return to the court* and request *identified* location data for the relevant devices supported by particularized probable cause for *each* device.[173] The following sections outline the appropriate Fourth Amendment standards for step one and step two data.

[166] *Id.*
[167] *Id.*
[168] Two of the three cases found the warrant to be constitutionally valid, but those courts noted that the good faith exception would apply if it were not valid. *See* United States v. Wright, No. CR419-149, 2023 WL 6566521, at *15 (S.D. Ga. May 25, 2023), *aff'd in part*, 2023 WL 5804161 (S.D. Ga. Sept. 7, 2023); United States v. Carpenter, No. 8:21-CR-309-VMC-MRM, 2023 WL 3352249, at *12 (M.D. Fla. Feb. 28, 2023); United States v. Smith, No. 3:21-CR-107-SA, 2023 WL 1930747, *10–12 (N.D. Miss. Feb. 10, 2023); United States v. Rhine, 652 F. Supp. 3d 38, 89–90 (D.D.C. 2023); United States v. Chatrie, 590 F. Supp. 3d 901, 937–41 (E.D. Va., 2022).
[169] Esteban De La Torre, *Digital Dragnets: How the Fourth Amendment Should be Interpreted and Applied to Geofence Warrants*, 31 SO. CAL. INTERDISC. L. J. 329, 347 (2022).
[170] *See supra* Part V(C), (F).
[171] *See Texas*, No. 2:22-mj-01325, 2023 WL 2236493, at *6 (S.D. Tex. Feb. 14, 2023); *DC*, 579 F. Supp. 3d 62, 88 (D.D.C. 2021).
[172] *See Texas*, 2023 WL 2236493, at *6; *DC*, 579 F. Supp. 3d at 88.
[173] *See Texas*, 2023 WL 2236493, at *6; *DC*, 579 F. Supp. 3d at 88–89.

b. A Reasonable Expectation of Privacy and the Third-Party Doctrine

As previously mentioned, a Fourth Amendment search occurs when the government "violates a subjective expectation of privacy that society recognizes as reasonable."[174] In the geofence warrant context, users *do not* have a reasonable expectation of privacy in step one data but *do* have a reasonable expectation of privacy in step two data.[175] In step one, law enforcement would receive anonymized data, which lacks personal identifiers.[176] This anonymization means the data does not infringe on specific individuals' privacy expectations, as it is nearly impossible to attribute the collected location data to a particular person.[177] Moreover, when geofence location data collection is limited by time, location, and scope, no one's "familial, political, professional, religious, [or] sexual associations . . ." could be discovered from the anonymous data.[178]

However, in step two of the geofence warrant process, where location data is linked to identifiable individuals, the dynamics of privacy expectations shift significantly. This transition from anonymity to identifiable data brings into play a reasonable expectation of privacy. At this stage, the data ceases to be a mere abstract location point and becomes a record of a specific individual's location and associations.[179] Although step-two location data will be limited by time, location, and scope, this personalized data has the potential to reveal intimate aspects of a person's life.[180] For example, a specific location point could indicate a person's visit to a sensitive location, such as a medical clinic, a political rally, or a religious institution. Moreover, research shows that 71% of American adults are concerned about how the government uses data it collects about them, indicating society recognizes an expectation of privacy in their data.[181] In this light, individuals have a reasonable expectation of privacy in step two data.

Furthermore, the third-party doctrine should only apply in the context of geofence warrants once companies provide transparent information about how user data is collected and used. Under the third-party doctrine, an individual surrenders a reasonable expectation of privacy in information voluntarily disclosed to others.[182] Since *Carpenter*,

---

[174] Kyllo v. United States, 533 U.S. 27, 33 (2001).
[175] This view is supported by *Texas*, 2023 WL 2236493, at *7–8; United States v. Rhine, 652 F. Supp. 3d 38, 83 n.22 (D.D.C. 2023); and *DC*, 579 F. Supp. 3d at 89 n.26.
[176] *See DC*, 579 F. Supp. 3d at 89 n.26.
[177] In certain circumstances, it is possible to reidentify anonymous data by linking anonymous data to other data or looking at unique characteristics found in the data. Latanya Sweeney, *K-Anonymity: A Model for Protecting Privacy,* 10 INT'L J. ON UNCERTAINTY, FUZZINESS & KNOWLEDGE-BASED SYS. 557, 558 (2002). For instance, the court in *Rhine* indicated that reidentification could happen by "cross-referencing more revealing location points—for example, the location where the device spent the night." *Rhine*, 652 F. Supp. 3d at 83 n.22. However, reidentification would be near impossible when the two-step process is followed because proper time, location, and scope limitations would eliminate the chance of reidentification by reducing the amount of geofence location data collected such that law enforcement could not, for example, learn where a data point stays overnight. *See id.*
[178] *Texas*, 2023 WL 2236493 at *8.
[179] *See DC*, 579 F. Supp. 3d at 89 n.26.
[180] *See* NACDL Fourth Amendment Center, *Geofence Warrant Primer*, NACDL, https://www.nacdl.org/getattachment/816437c7-8943-425c-9b3b-4faf7da24bba/nacdl-geofence-primer.pdf (last visited Feb. 8, 2024).
[181] *How Americans View Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.
[182] *Supra* Part IV(A)(2).

societal norms and expectations around privacy have evolved.[183] Notably, 74% of adults think it is acceptable for law enforcement to use information from cell phone towers to track where someone is.[184] Moreover, it is common knowledge today that location data is routinely collected, stored, and used for business purposes by third parties, such as big tech companies, social media platforms, and various apps. Indeed, research shows that 72% of American adults recognize "all, almost all or most of what they do online or while using their cellphone is being tracked by advertisers, technology firms or other companies," and that when it comes to offline behavior, such as their location, 69% believe companies are tracking some of that activity.[185]

Nevertheless, the complexity of the third-party doctrine arises from the nature of user agreements and privacy policies, which are often lengthy, complex, and not thoroughly read by users. Location data cannot be truly voluntarily shared with third parties when only one-in-five adults always or often read privacy policies, leaving four-in-five always or sometimes skipping privacy policies.[186] Further, 81% of Americans believe they have no control over the data companies collect about them and 59% have little to no understanding about what companies do with the data collected.[187] Just as the court reasoned in *Chatrie*, users cannot voluntarily disclose location data when there are limited and vague warnings.[188] Thus, until there is a societal shift towards transparent and comprehensible data collection policies, as well as a demonstrable understanding by users of these policies, the third-party doctrine should not apply to geofence warrants.

c. Step One Warrant Standards

i. Probable Cause

The geofence warrant probable cause standard at the first step involves two key components: (1) a fair probability that a crime has occurred, and (2) a fair probability that the identity of the perpetrator or witnesses of that crime will be encompassed within the search of the company's servers.[189]

The cases discussed in Part V show that law enforcement can establish the first requirement through evidence and observations establishing specific facts indicating a crime occurred. This can be through direct or circumstantial evidence, such as

[183] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so 'for any extended period of time was difficult and costly and therefore rarely undertaken.' For that reason, 'society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.' Allowing government access to cell-site records contravenes that expectation." (quoting United States v. Jones, 565 U.S. 400, 429-30 (2012) (Alito, J., concurring)).
[184] *See* Colleen McClain et al., *1. Views of Data Privacy Risks, Personal Data and Digital Privacy Laws*, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/.
[185] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
[186] *See id.*
[187] *Id.*
[188] *Supra* Part V(D).
[189] *Texas*, 2023 WL 2236493 at *8–9.

surveillance footage showing a crime in progress, eyewitness accounts, or other forms of proof.

To meet the second requirement, sufficient evidence must demonstrate a nexus between the criminal activity and the search of the company's servers.[190] To show this nexus, the cases discussed in Part V indicate that the geofence warrant application must indicate a fair probability that (i) the perpetrators or witnesses were inside the geofence and (ii) were possessing or using their cell phones inside the geofence, such that it would (iii) communicate location information to the company.[191]

To meet the first element, the geofence location and time frame must contain the area of the criminal activity during the time the crime occurred.[192] Law enforcement can meet this requirement through direct evidence, such as video footage with timestamps showing the suspects at the crime scene, or circumstantial evidence that allows the judge to make reasonable interferences, such as an explanation that the suspects would likely be in a portion of the geofence in order to access the crime scene.[193]

The second element—a fair probability the suspects or witnesses were using or possessing a cell phone—can likewise be established through direct evidence and circumstantial evidence.[194] Direct evidence can be straightforward, such as video surveillance showing relevant individuals actively using their cell phones.[195] However, in many scenarios, direct evidence might not be available. This is where circumstantial evidence, supported by an officer's training and experience, plays a vital role. The very nature of certain crimes might implicitly suggest the use of mobile devices. For example, it would be sufficient for law enforcement to assert that based on typical patterns of criminal behavior, co-conspirators often communicate by cell phone during the crime.[196] In crimes where it is likely a lone individual committed the crime, law enforcement can bolster their support by incorporating witnesses in its reasoning. Initially, law enforcement could assert that, based on experience, "it is rare to search an individual in the modern age during the commission of a crime and not find a cell phone on the person."[197] Then, law enforcement might reason that given the ubiquity of cell phones in contemporary society,[198] it is unlikely for individuals within the geofence—whether involved in the crime or as bystanders—not to possess a cell phone.

Finally, law enforcement must explain how and why cell phones may contain location data evidence, supported by an agent's training and experience, to establish the third element—that there is a *fair probability* a cell phone communicated location data to the

[190] *See DC*, 579 F. Supp. 3d 62, 75 (D.D.C. 2021).
[191] *See, e.g., id.* at 77–79.
[192] *Id.* at 82.
[193] In *DC*, there was direct evidence—the suspects were seen on videotape inside the area of the crime—and circumstantial evidence—the court reasonably inferred the suspects would likely access the crime scene from the adjoining parking lot. *Id.* at 77–78.
[194] *See id.* at 78 (finding that even though there was direct evidence the suspects were using cell phones, direct evidence was not necessary because "it is eminently reasonable to assume that criminals, like the rest of society, possess and use cell phones to go about their daily business.").
[195] *See* United States v. Rhine, 652 F. Supp. 3d 38, 85 (D.D.C. 2023); *Texas*, No. 2:22-mj-01325, 2023 WL 2236493, at *2 (S.D. Tex. Feb. 14, 2023).
[196] *See Arson Investigation*, 497 F. Supp. 3d 345, 356 (N.D. Ill. 2020).
[197] *Id.*
[198] *See id.* (asserting that the "ubiquity of cell phones and their common usage [has been] aptly describe[d] by the Supreme Court . . . .").

company.[199] Meeting this element depends on which company the geofence warrant is targeting and, after Google's new Location History policy,[200] may be a tough element to meet. To protect society from law enforcement pursuing geofence warrants in any case they wish, law enforcement must explain how various smartphones share location data with these companies, including through their operating systems and applications.[201] The affidavit should describe common location data collection practices, such as GPS, cell-site towers, Wi-Fi, and Bluetooth, and how these methods apply to the targeted company.[202] It should also address smartphones' ubiquity in the company's services or applications.[203]

ii. Particularity

The first step geofence warrant particularity standard includes three elements: (i) the warrant must identify the location to be searched (i.e., the company's servers), (ii) it must describe the geofence location and time frame with specific particularity, and (iii) it must identify what data to seize.[204] Each of the three elements is straightforward to meet. The first element merely requires stating which company's servers will be searched; it does not require stating exactly where those servers are located.[205] For the second element, the inquiry is simply whether the geofence location encompasses the area of the crime and whether the time frame covers the time the crime occurred.[206] The size of the geofence area and length of the time frame are a question of overbreadth, a consideration separate from particularity.[207] For the third element, absolute precision is not required when describing the type of location data to be seized.[208] Instead, "what is realistic or possible for [geofence warrants] . . ." is a generic description of seizing location data associated with "the investigation at hand."[209]

iii. Overbreadth

Overbreadth deals with the requirement that the location data to be seized must not be "broader than the probable cause on which it is based."[210] The goal of this requirement is to avoid capturing data of unrelated individuals. First, the time frame must show a close nexus to the criminal activity, encompassing only the duration of the crime or a reasonable

[199] Probability is the key consideration, not certainty. *Id.*
[200] *See* Part III(A).
[201] *See, e.g., DC*, 579 F. Supp. 3d 62, 78 (D.D.C. 2021) (asserting that "[r]oughly three-quarters of all phones worldwide contain Google's OS, and even those phones without Google's OS nonetheless have access to popular Google applications, the use of which can cause location information to be transmitted to Google.").
[202] *See id.* at 69–71.
[203] *Id*. at 70–71. For example, if the geofence warrant targets Microsoft, the application must describe how Microsoft collects location data, how such data is transmitted to the company's servers, and the ubiquity of a user using a Microsoft platform that collects location data. *See, e.g., id.* at 69–71.
[204] *Texas*, No. 2:22-mj-01325, 2023 WL 2236493, at *10–11 (S.D. Tex. Feb. 14, 2023).
[205] *See id.* at *10.
[206] *See id.* at *10–11.
[207] *Id.* at *10.
[208] *Arson Investigation*, 497 F. Supp. 3d 345, 357 (N.D. Ill. 2020).
[209] *Id.*
[210] United States v. Chatrie, 590 F. Supp. 3d 901, 928 (E.D. Va. 2022) (citing United States v. Hurwitz, 459 F.3d 463, 473 (4th Cir. 2006)).

and justified period before and after the crime.[211] Similarly, the geofence location must be strictly limited to the crime scene and its access areas, avoiding including nearby public spaces.[212]

Moreover, law enforcement must explain their parameters, supported by thorough investigations, to assure the court that the data captured will likely only include relevant individuals.[213] For example, suppose the geofence area encompasses a street leading to the crime scene. In that case, law enforcement can employ subsequent investigation—such as surveillance to determine whether the street is busy at the time of the crime—to justify that including it will not result in collecting large amounts of location data for uninvolved individuals. Similarly, suppose law enforcement employs a narrowing technique using a primary and control list, as in *Rhine* and *Texas*.[214] In that case, it must state that it is collecting location data for a time period extending beyond the time of the crime to eliminate uninvolved individuals from step two data collection.

d. Step Two Warrant Standards

In the second step of the geofence warrant process, law enforcement must return to the court for authorization before obtaining identifiable location data.[215] This step involves meticulously analyzing the anonymized data obtained in step one.[216] Law enforcement must analyze the step one anonymous location data and determine, based on the movement of the devices through the geofence area[217] or the location of the devices at particular time,[218] which devices could belong to the suspect or witnesses. Any devices irrelevant to the investigation must be excluded from the request for identified data.[219] This targeted analysis is essential for establishing particularized probable cause for each device for which identifiable information is sought while mitigating overbreadth concerns by ensuring that only data pertaining to individuals likely involved in the crime is made identifiable.[220]

---

[211] For instance, law enforcement in *Texas* aligned the time frame with moments of unauthorized withdrawals to ensure relevance and minimize overreach. *Texas*, 2023 WL 2236493, at *11–13.
[212] For example, law enforcement in *Rhine* contoured the geofence around the Capitol building and excluded nearby plazas. United States v. Rhine, 652 F. Supp. 3d 38, 86–87 (D.D.C. 2023).
[213] *Kansas*, 542 F. Supp. 3d 1153, 1158 (D. Kan. 2021); *Arson Investigation*, 497 F. Supp. 3d at 358–59.
[214] *Rhine*, 652 F. Supp. 3d at 69, 85–86 (utilizing a control list and primary list of devices to eliminate uninvolved devices); *Texas*, 2023 WL 2236493, at *12 (requesting data "stretch[ing] a few minutes after each unauthorized withdrawal" to "reduce overcollection of information.").
[215] *Texas*, 2023 WL 2236493, at *6; *DC*, 579 F. Supp. 3d 62, at 8889 (D.D.C. 2021).
[216] *See DC*, 579 F. Supp. 3d at 73.
[217] The *DC* opinion illustrates that law enforcement can narrow the relevant devices by examining the movement of devices across the geofence location and eliminating devices that move in a manner inconsistent with the facts of the case. *Id.*
[218] *Rhine* illustrates an effective narrowing technique that reduced the number of devices for which identified data would be revealed by incorporating a control list and primary list of location data. The control list only included devices that fell inside the geofence area but outside the geofence time frame while the primary list only included devices that fell within the geofence area inside the geofence time frame. The point of the two separate lists was to remove any devices that appeared on both lists because those who were inside the Capitol building before or after the criminal activity were lawfully inside the building. Thus, the remaining devices were, with a fair probability, suspects of the crime. *Rhine*, 652 F. Supp. 3d at 69, 85–86.
[219] *See id.*
[220] *See id.*

Consequently, step two serves as a vital filter, aligning the search with Fourth Amendment standards by focusing on particularized probable cause. This not only safeguards the privacy of uninvolved individuals, but also reinforces the constitutional integrity of the search.

VII. Conclusion

In conclusion, this Note navigated the intricate legal terrains of geofence warrants, analyzing company policies, the Fourth Amendment, and federal opinions to illuminate the balance between privacy rights and law enforcement efficacy. This analysis shows the balance between protecting individual privacy and enabling effective law enforcement is delicate and evolving. Despite Google's policy changes for Location History data storage, these warrants remain relevant due to the ongoing collection of vast amounts of location data by other tech companies and the other methods in which Google collects location data.

This Note recommends courts adopt a nuanced approach that safeguards individuals' reasonable expectation of privacy while still allowing law enforcement to harness the potential of location data in criminal investigations. To achieve this balance, the following measures should be implemented. First, a clearly defined and consistently applied probable cause standard requires law enforcement to demonstrate a specific nexus between the crime being investigated and the location data sought through geofence warrants. Second, a stringent particularity requirement ensures geofence warrants define the geographic area and the time frame of the data request. Lastly, overbreadth concerns must be addressed by limiting the scope of data collected by ensuring the time, location, and overall scope of the search are consistent with the probable cause set forth in the warrant application—minimizing the impact on innocent individuals' privacy.

With the two-step framework and a defined particularized probable cause standard, it is possible to strike a balance that upholds the fundamental principles of the Fourth Amendment, while still empowering law enforcement to utilize geofence warrants as a valuable tool in the pursuit of justice. This approach promotes a more equitable and just legal framework that respects privacy rights while addressing the unique challenges posed by emerging technologies and the ever-changing digital landscape.