PRIVACY AT THE PERIMETER: A CASE FOR A FILTER-FOCUSED APPROACH TO GEOFENCE WARRANTS ACROSS A DIVIDED JUDICIARY

Carissa R. Patton*

Tracking your every move: a substantial invasion of privacy, yet a highly effective way to locate potential suspects. The Fourth Amendment exists to protect the privacy of individuals from government intrusion, but courts have little guidance on how it applies in a world of emerging technology—technology such as geofences, which can track a person's location in immense detail. As a result, judges have differed profoundly in their analyses of how the Fourth Amendment applies to warrants for geofence location data. In July 2024, in the original United States v. Chatrie *decision, the Fourth Circuit found that individuals do not have a reasonable expectation of privacy in their geofence location data, and as a result, no warrant is required for law enforcement to obtain that data. One month later, a split emerged after the Fifth Circuit, in* United States v. Smith*, found that individuals have a reasonable expectation of privacy in their geofence location data and, additionally, that geofence warrants are unconstitutional general warrants. Considering the vastly different views, this Note proposes a middle ground between the original Fourth Circuit opinion and the Fifth Circuit opinion—a filter-focused approach to geofence warrants, which would help protect the privacy of individuals within geofence perimeters while facilitating effective policing.*

TABLE OF CONTENTS

INTRODUCTION 1154

I. BACKGROUND 1157
A. Understanding Geofence Warrants 1157
B. Understanding Google's Location Data and Geofence Warrant Policies .1158

II. HISTORY OF THE RELEVANT LAW 1162

---

* J.D. Candidate, University of Arizona James E. Rogers College of Law, 2026. I am deeply grateful to Professor Andrew Woods for sparking my interest in privacy law and for being an insightful and encouraging faculty advisor. I would also like to thank Professors Tessa Dysart and Diana Simon for developing my legal writing, Dean Jason Kreag for his constant willingness to answer "one more question" about the Fourth Amendment, and my wonderful peers at *Arizona Law Review* for their help at every stage of the writing process. Finally, thank you to my family and friends for your endless love and support.

A. The Fourth Amendment and Its Requirements 1163
B. Development of Fourth Amendment Case Law 1163
1. The Location Tracking Cases 1164
2. The Third-Party Doctrine Cases 1164
C. Lower Court Concerns About Geofence Warrants 1166
1. Lack of Additional Judicial Action Before Deanonymization 1166
2. Unbridled Discretion to Law Enforcement 1168
3. Potential to Obtain Data from Innocent Individuals 1168

III. THREE POTENTIAL CONCLUSIONS ON GEOFENCE WARRANTS: ALWAYS, NEVER, OR SOMETIMES ALLOW THEM 1169
A. Geofence Warrants Never Required 1170
B. Reverse Warrants Never Allowed 1171
C. Reverse Warrants Allowed with a Sufficient Filter 1172

IV. REASONABLE EXPECTATION OF PRIVACY IN GEOFENCE LOCATION DATA 1173
A. Large Quantities of Highly Invasive Data 1175
B. Potential to Intrude on Constitutionally Protected Areas 1176
C. The "Voluntariness" of the Electronic Opt-In Process 1178
D. Summary of Points 1179

V. PROPERLY CONSTRAINED REVERSE WARRANTS AND GENERAL WARRANTS 1180
A. Conflicts with Precedent 1180
B. Distinctions from General Warrants 1182
C. Sufficiency of Warrants to Make Geofence Searches Reasonable 1183
D. Public Policy Support 1183
E. Prevention of Negative Alternatives 1184
F. Summary of Points 1185

VI. ALLOWING REVERSE WARRANTS WHEN COURTS HAVE DISCRETION TO DEANONYMIZE DATA AND APPROPRIATE FILTERING MECHANISMS ARE IN PLACE 1185
A. Reasonable Expectation of Privacy in Geofence Location Data 1186
B. Additional Probable Cause Showing Prior to Deanonymization 1187
C. Filtering Mechanism Requirement for Reverse Warrants 1187

CONCLUSION 1188

INTRODUCTION

"I was using an app to see how many miles I rode my bike and now it was putting me at the scene of the crime. And I was the lead suspect."[1] Zachary McCoy had ridden his bike in front of a home on the night it was burglarized—a seemingly inconsequential act—and yet he had to retain a lawyer and spend several thousand dollars to persuade police that he was innocent of the crime.[2] Local police had received a geofence warrant for all devices using Google's services in the area near

1. Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect.*, NBC NEWS (Mar. 7, 2020, at 04:22 MT), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/8JHS-52T6].

2. *Id.*

the burglarized home, and this warrant had scooped up data from McCoy, an innocent individual—a risk that "Google itself has described as 'a significant incursion on privacy.'"[3] After McCoy received an email that informed him that "local police had demanded information related to his Google account,"[4] he realized that the exercise-tracking app that he used to record his bike rides "relied on his phone's location services, which fed his movements to Google" and placed him at the scene of the crime.[5] McCoy never realized that law enforcement could obtain this tracking information, but the email put him on notice so that he could retain a lawyer.[6] With the help of an attorney, McCoy avoided being detained for a crime he did not commit, but other innocent individuals who have become suspects because of a geofence warrant have not been as fortunate.[7]

Data-driven policing has become more prevalent over the years, and it utilizes several different types of data, including the following: (1) current and historical crime reports and incident data; (2) demographic information about the community; (3) geographic and spatial data about the community; (4) open-source intelligence including social media and public records; and (5) sensor data, including data picked up from traffic cameras.[8] As a result, law enforcement has begun using reverse search warrants—warrants that allow law enforcement to collect data to identify a suspect.[9] Geofence warrants are just one example of reverse search warrants, with other examples including tower dump dragnets,[10] keyword

---

3. *Id.*; Geofence warrants seek "cell phone location information that is stored by third-party companies," and they identify "everyone at a location (provided that they have a cell phone and it is turned on) during a particular time." Brian L. Owsley, *The Best Offense is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 HOFSTRA L. REV. 829, 833 (2022).

4. Schuppe, *supra* note 1.

5. *Id.*

6. *Id.*

7. *Id.*; 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/UX2E-FWRY].

8. *Data-Driven Policing: Enhancing Work with Analytics*, THOMSON REUTERS (Oct. 4, 2024), https://legal.thomsonreuters.com/blog/data-driven-policing-enhancing-work-with-analytics/ [https://perma.cc/7MJE-E5KS] ("Another milestone in the development of data-driven policing was reached in 2011 when the Los Angeles Police Department implemented its Operation LASER and PredPol policing software.").

9. Reverse search warrants are "searches used to find suspects and are not conducted to find evidence on a targeted individual." *Reverse Search Warrants*, NAT'L ASS'N CRIM. DEF. LAWS., https://www.nacdl.org/Landing/Reverse-Search-Warrants [https://perma.cc/XY8D-B8HU] (last visited Oct. 21, 2025). By "allowing police to discover who the suspect is rather than requiring police to come with a suspect in mind," these reverse warrants "limit[] the discretion of the police to select their targets in advance." Jane R. Bambauer, *Filtered Dragnets and the Anti-Authoritarian Fourth Amendment*, 97 S. CAL. L. REV. 571, 609–10 (2024).

10. *See* Carpenter v. United States, 585 U.S. 296, 316 (2018) (describing tower dumps as "a download of information on all the devices that connected to a particular cell site during a particular interval"); Bambauer, *supra* note 9, at 574 (explaining how standard dragnets "permit[] law enforcement to observe large amounts of data and to choose their targets. . . .").

search warrants, DNA database warrants, and credit card data warrants;[11] but courts will likely analyze all data from the above categories in the same way.[12] In fact, courts have already started using reasoning from geofence cases in cases involving tower dumps and keyword search history warrants.[13] As a result, while courts are currently analyzing issues relating to geofence warrants, the impacts of these decisions will be tremendous and encompass "most law enforcement and national security surveillance involving the Internet."[14]

After the first geofence warrant request in 2016, the number of requests for geofence warrants and geofence data has skyrocketed.[15] Because more cases have involved geofence warrants in recent years, courts have begun trying to answer the legal questions posed by geofence warrants and their associated data.[16] In 2024,

---

11. Ishe Marathe, *Circuit Split Over Geofence Warrants Could Have Major Fourth Amendment Implications for Data Searches*, LAW.COM (Aug. 29, 2024, at 20:38 MT), https://www.law.com/legaltechnews/2024/08/29/circuit-split-over-geofence-warrants-could-have-major-fourth-amendment-implications-for-data-searches/?slreturn=20240730143816 [https://perma.cc/CNJ2-WNYN].

12. *See* Bambauer, *supra* note 9, at 599 (applying Fourth Amendment principles to filtered dragnets—including at least geofencing and reverse keywords searches—and discussing that courts and scholars should recognize that filtered dragnets in general are consistent with Fourth Amendment principles); Orin S. Kerr, *Data Scanning and the Fourth Amendment* 2 (Mar. 31, 2025) (Stan. L. Sch., Pub. L. & Legal Theory Rsch. Paper Series Working Paper) (noting that courts have found that the Fourth Amendment covers "compelled access to database records of Google search terms, geofencing records, and tower dumps"); *id.* at 18–21 (noting that the principles used in the legal analysis for geofences in *Smith* can apply more broadly); *id.* at 42–46 (applying a filter-focused approach to data scanning situations including geofencing, email scans, and reverse keyword searches).

13. *In re* Four Applications for Search Warrants Seeking Info. Associated with Particular Cellular Towers, No. 3:25-CR-38-CWR-ASH, 2025 WL 603000, at *4–8 (S.D. Miss. Feb. 21, 2025); Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2529 (2021).

14. Orin S. Kerr, *The Fifth Circuit Shuts Down Geofence Warrants—And Maybe A Lot More*, REASON (Aug. 13, 2024, at 05:28 MT), https://reason.com/volokh/2024/08/13/fifth-circuit-shuts-down-geofence-warrants-and-maybe-a-lot-more/ [https://perma.cc/AQB4-RVFS].

15. *Global Requests for User Information*, GOOGLE, https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period [https://perma.cc/H2X8-F9S8] (last visited Oct. 15, 2025); Jennifer Lynch, *Modern-Day General Warrants and the Challenge of Protecting Third-Party Privacy Rights in Mass, Suspicionless Searches of Consumer Database*, HOOVER INST. 1, 5 (Sep. 23, 2021), https://www.hoover.org/sites/default/files/research/docs/lynch_webreadypdf.pdf [https://perma.cc/PDE6-W79X].

16. *See, e.g.*, *In re* Search of Info. Stored at Premises Controlled by Google, as further described in Attachment A, No. 20 M 297, 2020 WL 5491763, at *7 (N.D. Ill. July 8, 2020); *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 349 (N.D. Ill. 2020); *In re* Search of Info. that Is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 90–91 (D.D.C. 2021).

circuit courts began publishing decisions involving geofence warrants, but after three decisions and one month's time, a circuit split emerged.[17]

This Note will illustrate why courts should take a filter-focused approach to analyzing reverse warrants, such as geofence warrants. First, it will provide a background on geofence warrants and Google's policies for responding to the geofence requests. Then, it will discuss the history of relevant Fourth Amendment case law and provide a high-level overview of various district court cases involving geofence warrants. Next, it will explain the court divide—including the original Fourth Circuit opinion on geofence warrants, the Fifth Circuit opinion on geofence warrants, and the Colorado and Georgia Supreme Court cases on reverse warrants. Finally, this Note will argue that courts should recognize a reasonable expectation of privacy for the location data used in geofences and should require law enforcement to obtain a warrant to reach this data. Further, courts ought to use a filter-focused approach and allow reverse warrants when there is a sufficient filter in place.

I. BACKGROUND

A. Understanding Geofence Warrants

Over the years, law enforcement has started using digital technology in new ways—such as seeking access to location data using geofence warrants. Originally, geofencing was used to create a virtual "fence" that could provide targeted ads when users were near certain locations or alert law enforcement whenever a person left a predefined perimeter.[18] In 2016, law enforcement started applying for geofence search warrants, combining the concept of the virtual perimeter with a traditional search warrant.[19] Geofence warrants are different from typical search warrants

17. *See generally* United States v. Chatrie, 107 F.4th 319 (4th Cir. 2024) (analyzing a geofence warrant); United States v. Davis, 109 F.4th 1320 (11th Cir. 2024) (same); United States v. Smith, 110 F.4th 817 (5th Cir. 2024) (same). In April of 2025, an en banc Fourth Circuit court issued a one-line per curiam opinion affirming the judgment of the district court—vacating the much longer original opinion, which also affirmed the district court's decision. United States v. Chatrie, 136 F.4th 100, 100 (4th Cir. 2025) (en banc). Instead of creating a "Fourth Amendment compass," the 2025 *Chatrie* opinion offered "a labyrinth of—by [the Chief Judge's] count, nine—advisory opinions, many pointing in different directions." *Id.* at 108–09 (Diaz, C.J., concurring). Six of the fifteen judges joined Judge Richardson's concurrence, which included reasoning that was identical to the original 2024 decision—a decision authored by Judge Richardson. *Id.* at 130–41 (Richardson, J., concurring). In his concurrence, Judge Richardson found that the government did not conduct a search when it obtained Chatrie's Location History data. *Id.* at 138–39. In contrast, another six judges wrote or joined opinions that concluded the government did conduct a Fourth Amendment search by collecting Chatrie's Location History information. *Id.* at 115 (Wynn, J., concurring); *id.* at 156 (Berner, J., concurring). Given this fragmentation, it is hard to determine how the Fourth Circuit might resolve similar cases in the future. Regardless, the original 2024 decision is representative of an analysis a court might use when analyzing geofence warrants, so it is helpful to discuss that opinion in this Note.

18. People v. Meza, 312 Cal. Rptr. 3d 1, 6 (Cal. Ct. App. 2023); Owsley, *supra* note 3, at 832–33; United States v. Cabrera, No. 11-117-GMS, 2014 WL 3540894, at *3 (D. Del. July 15, 2014).

19. Owsley, *supra* note 3, at 832–33.

because they do not identify "a specific person, device, or account" but rather specify a geographical area and a time period so that law enforcement can work in "reverse" by starting with the crime rather than a suspect.[20] Law enforcement uses these warrants to require third-party companies to search all of their user data to find all the users who fit the parameters provided.[21] While these expansive requests potentially expose the data of hundreds—if not thousands—of individuals, they rarely lead to the arrests of suspects,[22] and they have been overused in "run-of-the-mill cases that present no urgency or imminent danger."[23] Further, judges usually seal geofence warrants, so it is hard to know exactly how judges analyze them.[24] Some judges have hastily granted geofence warrants without ever seeing a map of the requested area or requiring the warrant applications to "spell out plainly the area covered by the warrant, what was inside the targeted areas, or how the areas were related to the crime at all."[25] As a result of these geofence warrants, there are numerous documented false positives of "innocent bystanders being swept into geofence warrants" solely because they were near a crime.[26]

B. Understanding Google's Location Data and Geofence Warrant Policies

Nearly all geofence requests have targeted Google, and the requests have increased exponentially over the last several years.[27] Since Google has the ability to

---

20. Lynch, *supra* note 15, at 4.

21. *Id.*

22. Stephen Silver, *Police are Casting a Wide Net into the Deep Pool of Google User Location Data to Solve Crimes*, APPLEINSIDER (Mar. 19, 2018, at 09:52 ET), https://appleinsider.com/articles/18/03/19/police-are-casting-a-wide-net-into-the-deep-pool-of-google-user-location-data-to-solve-crimes [https://perma.cc/WRZ9-QVWM] (noting that "[o]nly one of the four cases that sought Google geofencing data has resulted in an arrest").

23. Jennifer Lynch & Nathaniel Sobel, *New Federal Court Rulings Find Geofence Warrants Unconstitutional*, ELEC. FRONTIER FOUND. (Aug. 31, 2020), https://www.eff.org/deeplinks/2020/08/new-federal-court-rulings-find-geofence-warrants-unconstitutional-0 [https://perma.cc/5DS2-YUCD] (quoting *In re* Search of Info. Stored at Premises Controlled by Google, as further described in Attachment A, No. 20 M 297, 2020 WL 5491763, at *8 (N.D. Ill. July 8, 2020)); Tony Webster, *How Did the Police Know You Were Near a Crime Scene? Google Told Them*, MPR NEWS (Feb. 7, 2019, at 15:10 MT), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants [https://perma.cc/6ZZ4-7Q84] (noting that "police have used the warrants in cases to find suspects who stole a pickup truck" and who "broke into a Fleet Farm store to steal tires"); *In re* Search of Info. Stored at Premises Controlled by Google, as further described in Attachment A, No. 20 M 297, 2020 WL 5491763, at *8 (N.D. Ill. July 8, 2020).

24. Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2514 (2021) (explaining that the secrecy in geofence warrants prevents the "public from knowing how judges consider these warrants and whether courts have been consistent").

25. *See* Webster, *supra* note 23.

26. United States v. Smith, 110 F.4th 817, 825–26 (5th Cir. 2024).

27. Cyrus Farviar & Thomas Brewster, *Google Just Killed Warrants That Give Police Access to Location Data*, FORBES (Dec. 14, 2023, at 17:43 ET), https://www.forbes.com/sites/cyrusfarivar/2023/12/14/google-just-killed-geofence-warrants-police-location-data/ [https://perma.cc/26TK-NXYJ]. To see other companies' policies in responding to geofence warrants, see Emily Brodner, *Navigating the Terrain of Geofence Warrants*, 7 ARIZ. L.J. EMERGING TECH. 2, 4–5 (2024) (describing the policies for Lyft, Uber, Microsoft, and Yahoo).

gain location data on most cellphone users, it is easy to see why law enforcement has targeted the company for these warrant requests.[28] Google received its first geofence warrant request in 2016, and there was an over "1,500% increase in the number of geofence requests it received in 2018 compared to 2017."[29] Between 2018 and 2020, Google received approximately 20,000 geofence warrant requests—constituting more than a quarter of the total number of all warrant requests the company has ever received[30]—and it received as many as 180 geofence warrant requests within a single week.[31]

Google collects "detailed location data on 'numerous tens of millions' of its users," going back almost a decade, through its Location History, Web and App Activity, and Google Location Accuracy services.[32] Location History is "the most sweeping, granular, and comprehensive tool" when it comes to the collection and storage of location data, as it can draw from Global Positioning System ("GPS") information, Bluetooth beacons, cellphone location information from nearby cellular towers, internet protocol address information, and the signal strength of nearby Wi-Fi networks.[33] It is so granular that it can locate an individual within about 60 feet and can even determine what floor of a building an individual is on.[34] This service logs a device's location approximately every two minutes, and it supports Google's advertising revenue by "providing 'store visit conversions' or 'ads measurement' to businesses based on user location."[35] Once a user opts into Location History, Google is "always collecting" and storing that user's data in its database as it tracks a user's location "across every *app* and every *device* associated with the user's account."[36] In responding to geofence warrants, Google primarily uses its Location History data service because it collects enough data points to most accurately pinpoint devices within the geographic radius during a specific period of time.[37]

Google claims that before it starts tracking someone's location, a user must first opt into its Location History service,[38] but there are questions as to whether this

---

28. Specifically, Google Android devices—which comprise about 74% of the total smartphones worldwide—automatically have a Google Android operating system, and both Android and Apple cellular devices have "various Google apps that could potentially store a user's location" and "provide Google with a specific device's location." Owsley, *supra* note 3, at 834.

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

30. Lynch, *supra* note 15, at 5.

31. Valentino-DeVries, *supra* note 7.

32. *Chatrie*, 590 F. Supp. 3d at 907; Owsley, *supra* note 3, at 835.

33. *Chatrie*, 590 F. Supp. 3d at 907.

34. Owsley, *supra* note 3, at 835; *Chatrie*, 590 F. Supp. 3d at 908.

35. *Chatrie*, 590 F. Supp. 3d at 908.

36. *Id.* at 909.

37. *Id.* at 910.

38. *See Privacy & Terms*, GOOGLE, https://policies.google.com/technologies/location-data [https://perma.cc/GN2E-MNNN]; *Google Maps Help: Manage your Google Maps Timeline*, GOOGLE, https://support.google.com/maps/answer/6258979?hl=en&co=GENIE.Platform%3DAndroid [https://perma.cc/M79A-PFXK]; Matt Binder, *Google Tracks You Even if You Turn Off 'Location History': Report*, MASHABLE (Aug. 13,

"opting in" is truly voluntary.[39] A user must complete three steps to opt in: (1) turn on the device's device-location setting, (2) enable Location Reporting within the Location History service, and (3) log into his Google account on that device.[40] The Location History service appears voluntary, but most users likely do not realize that they are opting into this detailed location tracking,[41] and courts have expressed concerns as to whether an individual is actually in a "meaningful sense, . . . voluntarily '[assuming] the risk' of turning over a comprehensive dossier of his physical movements."[42] If users want to turn the Location History service off, that will prove challenging because "deactivating location history data based on Google's 'limited and partially hidden' warnings is 'difficult enough that people won't figure it out.'"[43]

Even if users successfully disable the Location History tracking, Google's terms of service inform users that the company "may still collect location data from searches or other apps."[44] But while Google says it "may" collect data, users should take this as a *promise* that Google will continue collecting their data.[45] For example, in Arizona, the Arizona Attorney General sued Google for collecting the location of

---

2018), https://mashable.com/article/google-location-history-tracking [https://perma.cc/RF43-8EW2].

39. *Chatrie*, 590 F. Supp. 3d at 936.

40. Owsley, *supra* note 3, at 837.

41. Schuppe, *supra* note 1 ("'I didn't realize that by having location services on that Google was also keeping a log of where I was going,' McCoy said. 'I'm sure it's in their terms of service but I never read through those walls of text, and I don't think most people do either.'"); 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/UWF4-HBYM].

42. *Chatrie*, 590 F. Supp. 3d at 936 ("While the Court recognizes that Google puts forth a consistent effort to ensure its users are informed about its use of their data, a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting 'YES, I'M IN' at midnight while setting up Google Assistant, even if some text offered warning along the way. The record here makes plain that these 'descriptive texts' are less than pellucid.").

43. Isha Marathe, *Tech Providers, Not Courts, May Have the Last Word on Geofence Warrants*, LAW.COM (Aug. 30, 2024, at 14:32 MT), https://www.law.com/legaltechnews/2024/08/30/tech-providers-not-courts-may-have-the-last-word-on-geofence-warrants/ [https://perma.cc/YTK7-H6W3] (quoting Google employees regarding how difficult it is to opt out of the service).

44. Skye Witley, *Google's Location Data Move Will Reshape Geofence Warrant Use*, BLOOMBERG L. (Dec. 20, 2023, at 03:05 MT), https://news.bloomberglaw.com/privacy-and-data-security/googles-location-data-move-will-reshape-geofence-warrant-use [https://perma.cc/LNZ9-6695].

45. *See* Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, ASSOCIATED PRESS (Aug. 13, 2018, at 17:15 MT), https://apnews.com/article/828aefab64d4411bac257a07c1af0ecb#:~:text=An%20Associated%20Press%20investigation%20found,findings%20at%20the%20AP's%20request [https://perma.cc/2E78-TPBW]; *see In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 737 n.3 (N.D. Ill. 2020) ("Published reports have indicated that many Google services on Android and Apple devices store the device users' location data even if the users seek to opt out of being tracked by activating a privacy setting that says it will prevent Google from storing the location data.").

its users even when they had turned off the Location History service.[46] Google used this tracking information to sell advertisements, and this suit ultimately resulted in an $85 million settlement that was the "largest amount per capita that Google has paid in a lawsuit about privacy and consumer fraud."[47] However, Google generated nearly 3,000 times this amount—$224 billion—*solely* from advertising revenue in the same year as the settlement.[48] Given this financial incentive, it is reasonable to conclude that Google may continue to track users without their consent even if users successfully turn their Location History service off.

In addition to the Location History service, Google has other ways to collect its users' locations, but it remains to be seen if law enforcement will be able to successfully access these other stores of location data on a mass basis for geofence warrants.[49] At the end of 2023, Google announced a policy change in how it will store Location History data, so law enforcement might not be able to continue using the Location History data for geofence warrants.[50] As this change rolls out to more users, there might be an answer in coming years as to which other Google services law enforcement will be able to successfully access in order to obtain individuals' location data.

Once the location data is collected, Google uses it to respond to geofence warrants using a three-step process.[51] At Step One, law enforcement must obtain a warrant to compel Google to provide an anonymous list of Google users whose Location History data placed them within the specified geographic area and timeframe.[52] In response, Google will search its entire user database to identify the devices present within the geofence.[53] Following the search, Google must provide the government with the corresponding records, including (1) deidentified device numbers, (2) "the latitude/longitude coordinates and timestamp of the stored [Location History] information," (3) the map's confidence interval, and (4) the

---

46. Angela Cordoba Perez & Jose R. Gonzales, *Google to Pay Arizona $85M in Privacy Suit That Alleged 'Deceptive' Location Tracking*, USA TODAY (Oct. 5, 2022, at 11:28 ET), https://www.usatoday.com/story/money/2022/10/05/google-arizona-lawsuit-settlment-85-million/8185226001/ [https://perma.cc/WK44-BWNS].

47. *Id.*

48. Tiago Bianchi, *Google: Annual Advertising Revenue 2001-2023*, STATISTA (May 22, 2023), https://www.statista.com/statistics/266249/advertising-revenue-of-google/ [https://perma.cc/8L3E-9C45].

49. Jennifer Lynch, *Is This the End of Geofence Warrants?*, ELEC. FRONTIER FOUND. (Dec. 13, 2023), https://www.eff.org/deeplinks/2023/12/end-geofence-warrants [https://perma.cc/5VZ2-MB7U].

50. 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/ [https://perma.cc/Z49D-AYWA]; Lars Daniel, *Google to Stop Giving Location Evidence to Law Enforcement*, FORBES (Oct. 8, 2024, at 11:50 ET), https://www.forbes.com/sites/larsdaniel/2024/10/08/google-to-stop-sharing-location-data-with-law-enforcement/ [https://perma.cc/4ZWD-SPR6].

51. Peter G. Berris & Clay Wild, *Geofence Warrants and the Fourth Amendment*, CONGRESS.GOV (May 9, 2025), https://www.congress.gov/crs-product/LSB11274 [https://perma.cc/QS6T-MTE6].

52. United States v. Chatrie, 590 F. Supp. 3d 901, 914–15 (E.D. Va. 2022).

53. *Id.*

Location History's source—specifically "whether the location was generated via Wi-Fi, GPS, or a cell tower."[54] While Google does not impose "specific, objective restraints" on the requested geographical area, the requested duration of time, or the number of users for which Google will provide data, Google does reserve the right to try to limit the request geographically or temporally.[55]

At Step Two, the government must review the anonymous data to determine "device numbers of interest."[56] At this point, law enforcement can compel Google to provide additional data beyond the geographic and temporal restraints of Step One to help narrow their investigation.[57] While Google does not impose any geographical constraints on Step Two data, Google does ostensibly require the government to reduce the number of users for which it requests data.[58] However, in the past, the government has failed to narrow the number of users and has instead requested additional information for all of the devices identified in Step One.[59]

At Step Three, Google will "provide account-identifying information" about the users that the government deems are relevant to the investigation.[60] While Google does not request that law enforcement obtain an additional court order prior to deanonymization, courts have often imposed this as an additional requirement so that discretion is left with courts and not with law enforcement.[61]

II. HISTORY OF THE RELEVANT LAW

Because courts are analyzing geofence cases under the Fourth Amendment, it is important to understand how Fourth Amendment jurisprudence has developed before applying it to the geofence context. Specifically, this Part will describe the Fourth Amendment, its requirements, and how courts have applied it in different contexts, including the geofence context.

---

54. *Id.* at 915.
55. *Id.*
56. *Id.* at 916.
57. *Id.*
58. *Id.*
59. *Id.* at 921 (noting that the detective "requested 'additional location data' (Step 2 data) and 'subscriber information' (Step 3 data) 'for all 19 device numbers produced in [S]tep 1'").
60. *Id.* at 916.
61. *Compare* United States v. Rhine, 652 F. Supp. 3d 38, 69, 88–89 (D.D.C. 2023) (finding the geofence warrant was constitutionally permissible and "did not vest too much authority in the Government" because the initial warrant "precluded disclosure of deanonymized device information except after a separate order of the court based on a supplemental affidavit"), *and Chatrie*, 590 F. Supp. 3d at 921 (noting that court authorization prior to deanonymization may render the geofence warrant constitutional), *with In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 362 (N.D. Ill. 2020) (finding that the government had sufficient probable cause for all location and subscriber data within the geofence at the initial step without any additional court order prior to deanonymization); *see* Berris & Wild, *supra* note 51.

A. The Fourth Amendment and Its Requirements

The Fourth Amendment protects the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[62] It further outlines that warrants require probable cause, supported by an oath or affirmation, and particularity as to "the place to be searched, and the persons or things to be seized."[63] Probable cause exists when there is "a fair probability that contraband or evidence of a crime will be found in a particular place."[64] Judges must analyze the totality of the circumstances to determine if this probable cause standard has been met.[65] In addition to probable cause, warrants must be particular, and this requirement exists to prevent general warrants[66]—warrants from the Colonial Era that gave officers "unfettered power" and allowed them to "rummage through homes in an unrestrained search for evidence of criminal activity."[67] Limiting the warrants with these two requirements helps ensure that the searches do not become "wide-ranging exploratory searches."[68]

B. Development of Fourth Amendment Case Law

As courts began applying the Fourth Amendment, a test quickly emerged for how to determine what was a "reasonable" search or seizure.[69] *Katz v. United States*, one of the first key cases in Fourth Amendment jurisprudence, established the reasonable expectation of privacy test, which requires that for a person to have a reasonable expectation of privacy, (1) the person must have a subjective expectation of privacy and (2) that expectation must be one that "society is prepared to recognize as 'reasonable.'"[70] This test guides courts when determining whether there was a Fourth Amendment violation, including in the contexts of tracking one's physical location or obtaining information from third parties—which are two of the most pertinent categories of cases for analyzing the Fourth Amendment implications of using geofences.[71]

---

62. U.S. CONST. amend. IV.
63. *Id.*
64. Illinois v. Gates, 462 U.S. 213, 238 (1983).
65. *Id.*
66. Maryland v. Garrison, 480 U.S. 79, 84 (1987).
67. *The Right to Be Secure: The Foundation of the Fourth Amendment*, INST. FOR JUST., https://ij.org/issues/ijs-project-on-the-4th-amendment/the-right-to-be-secure-the-foundation-of-the-fourth-amendment/ [https://perma.cc/BY6D-AE4A] (last visited Nov. 25, 2025); Riley v. California, 573 U.S. 373, 403 (2014); *see* Steagald v. United States, 451 U.S. 204, 220 (1981).
68. *Garrison*, 480 U.S. at 84.
69. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
70. *Id.*
71. *See* United States v. Chatrie, 590 F. Supp. 3d 901, 926, 935–36 (E.D. Va. 2022) (citing the third-party doctrine cases and the location tracking cases in its analysis); United States v. Rhine, 652 F. Supp. 3d 38, 81–82 (D.D.C. 2023) (same); United States v. Chatrie, 107 F.4th 319, 326–27 (4th Cir. 2024) (same); United States v. Brown, No. 1:16-CR-427-AT-JKL-31, 2025 WL 1674283, at *10–13 (N.D. Ga. June 13, 2025) (same).

1. The Location Tracking Cases

As Fourth Amendment case law developed, courts grappled with the issue of location tracking in the context of automobiles.[72] In *United States v. Knotts*, officers placed a tracker inside a container, ensured the container would be sold to the suspect, and tracked the automobile carrying the container to find the manufacturing location of illicit drugs.[73] The Court concluded that this was not a search because a person traveling in public has no reasonable expectation of privacy, but the Court also noted the government's "*limited use*" of the beeper occurred *solely* during the automobile journey.[74]

Similarly, in *United States v. Karo*, the Court considered a case in which law enforcement placed a tracker in a container that the suspects would unwittingly purchase so that the government could find and track the suspects.[75] However, in this case, the tracker was used in various private residences, so the Court concluded a search had occurred and a warrant was required.[76] Since the government did not know where the place to be searched would be, the government argued that it was "impossible to describe the 'place' to be searched."[77] But the Court rejected this argument and instead articulated a way to do it: describe (1) "the object into which the beeper is to be placed," (2) "the circumstances that led agents to wish to install the beeper," and (3) "the length of time for which beeper surveillance is requested."[78]

2. The Third-Party Doctrine Cases

Another line of cases relevant to the geofence warrant discussion is that of the third-party doctrine—a doctrine that allows law enforcement to collect evidence from third parties without a warrant in criminal cases.[79] Despite critiques from justices and scholars that the third-party doctrine does not "accurately apply" the *Katz* reasonable expectation of privacy test and that it gives the government too much power,[80] the doctrine is still valid law. This doctrine provides that individuals

---

72. United States v. Knotts, 460 U.S. 276, 278–79 (1983); United States v. Karo, 468 U.S. 705, 708–09 (1984); United States v. Jones, 565 U.S. 400, 403 (2012).

73. *Knotts*, 460 U.S. at 278–79.

74. *Id.* at 281, 284 (emphasis added).

75. *Karo*, 468 U.S. at 708–09.

76. *Id.* at 716.

77. *Id.* at 718.

78. *Id.*

79. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

80. *See* Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting) (expressing concern that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance"); Carpenter v. United States, 585 U.S. 296, 401 (2018) (Gorsuch, J., dissenting) ("Just because you have to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it."); Kerr, *supra* note 79, at 572 (describing the doctrinal critique that the third-party doctrine does not "accurately apply" the reasonable expectation of privacy test because individuals normally accept a lack of privacy in third-party records, especially when they have no reasonable alternative to using that service, and the functional critique that it grants the government unregulated power).

do not have a reasonable expectation of privacy in information that they voluntarily convey to third parties; instead, individuals accept the risk that the third party will convey their information to the government.[81] Established in the 1970s, the third-party doctrine was originally applied in the context of little to no technology, such as bank records or pen registers.[82] But despite "seismic shifts in digital technology" since these decisions,[83] the Supreme Court has not provided much guidance on how to apply the third-party doctrine to advanced technology.

In fact, the Supreme Court has rendered only one narrow decision regarding a specific type of technology.[84] Noting a "world of difference" from the "limited types of personal information" in cases previously decided under the third-party doctrine, the Supreme Court in *Carpenter v. United States* declined to extend the third-party doctrine to seven days of historical cell site location information ("CSLI")—time-stamped data collected by wireless carriers that is recorded whenever a phone connects to a cell site.[85] In 2011, the FBI obtained court orders that directed MetroPCS and Sprint to disclose CSLI records from the phone of a suspected robber, Timothy Carpenter.[86] Since phones are constantly searching for the best signal and connecting to different cell sites as a person moves, this CSLI data created a "detailed and comprehensive record of [Carpenter's] movements" and allowed law enforcement to create maps showing that Carpenter was near the location of four of six robberies at the time they were committed.[87]

The lower courts held that Carpenter lacked a reasonable expectation of privacy in the location information because "cell phone users voluntarily convey cell-site data to their carriers as 'a means of establishing communication,'" but the Supreme Court disagreed and carved out an exception to the third-party doctrine—albeit a "narrow one."[88] In explaining why the third-party doctrine would not extend to the seven days of historical CSLI data, the Court pointed to the revealing nature of CSLI, the amount of data collected, the number of people affected by a given surveillance program or practice, the inability to avoid collection of one's personal

---

81. United States v. Miller, 425 U.S. 435, 443 (1976).

82. *Id.* at 443; *Smith*, 442 U.S. at 744–45.

83. *Carpenter*, 585 U.S. at 309 ("After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."); *id.* at 313–14 ("The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years . . . . There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.").

84. *Id.* at 314.

85. *Id.* at 302, 310 n.3, 314–16 (noting that "*Smith* pointed out the limited capabilities of a pen register" and "[revealed] little in the way of 'identifying information'" and that the checks in *Miller* were "not confidential communications").

86. *Id.* at 302 (resulting in 127 days' worth of CSLI records from MetroPCS and 2 days' worth of CSLI records from Sprint).

87. *Id.* at 300–02, 309.

88. *Id.* at 303, 313, 316.

data, the automatic rather than voluntary nature of transmitting the data to a third party, and the cost of surveillance for government officials.[89]

C. Lower Court Concerns About Geofence Warrants

Geofence warrants were first used by law enforcement in 2016, and the first legal opinions about geofence warrants were published in 2020.[90] Before the circuit courts started hearing cases involving geofences, the district court cases focused on the sufficiency of the probable cause and particularity of the warrants themselves.[91] When analyzing these warrant requests and warrants, courts frequently expressed three major concerns: lack of additional judicial action before deanonymization, giving too much discretion to law enforcement, and exposing the data of innocent individuals.[92]

1. Lack of Additional Judicial Action Before Deanonymization

While Google follows a three-step process in responding to geofence warrants,[93] not all courts have approved of this protocol; rather, some have required court authorization prior to deanonymization of the data. For example, in *Search of Information that Is Stored at Premises Controlled by Google LLC*, the court took issue with the government's initially proposed three-step process that did not include any requirement for the government to return to the court prior to deanonymizing data.[94] The District Court for the District of Columbia had concerns with this protocol because of how much discretion it gave the government to order Google to disclose identifying information "without any guardrails on the exercise of that discretion or further review" by a court.[95] To overcome the overbreadth concerns, the government proposed two additional steps that would give the discretion to the court rather than to law enforcement: (1) the government will identify the devices for which it seeks identifying information "in additional legal process to the court," and (2) the court "*may then order*" Google to disclose the account-identifying

---

89. Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 HARV. L. REV. 1790, 1801–04 (2021) [hereinafter Tokson, *The Aftermath of* Carpenter].

90. Lynch, *supra* note 15, at 5; Donna Lee Elm, *Are Geofence Warrants Headed for Extinction?*, ABA CRIM. JUST., Summer 2024, at 48, 50 https://www.americanbar.org/groups/criminal_justice/resources/magazine/2024-summer/geofence-warrants-headed-extinction/ [https://perma.cc/7ZMA-H5TH]; *see generally In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345 (N.D. Ill. 2020) (analyzing a geofence warrant application).

91. *See In re* Search of Info. that Is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 73–74 (D.D.C. 2021); United States v. Easterday, 712 F. Supp. 3d 46, 51–54 (D.D.C. 2024).

92. While many cases discuss the three concerns listed when analyzing the warrant, portions of various cases are highlighted to give the clearest examples of each category. *See* Info. that Is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d at 73–74; *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 358 (N.D. Ill. 2020).

93. *See supra* Section I.B.

94. 579 F. Supp. 3d at 73.

95. *Id.*

information.[96] The court ultimately concluded that the scope of the warrant was constitutionally permissible in part because these two steps helped eliminate overbreadth concerns.[97] Similarly, in *United States v. Rhine*, the District Court for the District of Columbia concluded that a geofence warrant was sufficiently particularized because in order to obtain deanonymized information, law enforcement had to obtain a separate court order based on a supplemental affidavit—leaving the discretion ultimately with the court rather than the government.[98] The warrant proposed a three-step process: (1) Google provides the government with anonymized lists of devices—a primary list and two control lists; (2) the government reviews the lists to narrow down the devices of interest by using other investigative methods and by comparing against the control lists; and (3) the government identifies in a supplemental affidavit the devices for which it seeks identifying information, and the court has the discretion to order Google to disclose the information to the government after review of the supplemental affidavit.[99] Step Two's narrowing measures also helped ensure there was sufficient probable cause in the follow-up warrant affidavit,[100] ultimately leading to the court's holding that the warrant had the necessary particularized probable cause.[101]

Additionally, courts have deemed some two-step warrants acceptable when there is sufficient probable cause and courts, rather than the government, have the discretion to disclose identifying information.[102] In *Search of Information Stored at Premises Controlled by Google*, the District Court for the Southern District of Texas found that the warrant's two-step process protected against overbreadth since the "discretion regarding disclosure of identifiable data" would be exercised solely by the court.[103] The two steps included (1) Google identifying devices within the geofence in the given time period and providing the government with anonymized data and (2) law enforcement returning to the court "with one or more subsequent

96. *Id.* at 73–74.

97. *Id.* at 89–90.

98. 652 F. Supp. 3d 38, 68–69, 88–89 (D.D.C. 2023).

99. *Id.*; *see also* United States v. Easterday, 712 F. Supp. 3d 46, 49–50 (D.D.C. 2024) (noting the Magistrate Judge granted a warrant with a similar multi-step process).

100. *Rhine*, 652 F. Supp. 3d at 86.

101. *Id.* at 88–89.

102. *In re* Search of Info. Stored at Premises Controlled by Google, No. 2:22-MJ-01325, 2023 WL 2236493, at *6, *14 (S.D. Tex. Feb. 14, 2023) (granting the warrant request because there was "probable cause to believe that a crime has been committed," "that evidence of that crime will be found within the geofenced location that is the subject of this Step One warrant request," that the request was "sufficiently particular as to time, location, and scope" and "is not overbroad, because its proposed geographic area and time periods closely track the probable cause to justify the requested disclosure of information, and because it minimizes the likelihood that the Step One warrant will sweep up personally identifiable data of uninvolved persons"); United States v. Brown, No. 1:16-CR-427-AT-JKL-31, 2025 WL 1674283, at *15 (N.D. Ga. June 13, 2025) (finding that a geofence warrant lacked particularized probable cause and the "quantum of individualized suspicion" because there was "nothing in the First Warrant to limit the Government's ability to obtain identifying information for ***all*** devices within the geofence" since law enforcement did not make any additional probable cause showing at Step Two (emphasis added)).

103. *Search of Info. Stored at Premises Controlled by Google*, 2023 WL 2236493, at *13.

warrant requests," supported by probable cause, to obtain the deanonymized information.[104]

2. Unbridled Discretion to Law Enforcement

Similarly, courts have expressed concern about the particularity of geofence warrants when law enforcement, rather than the court, has the discretion to "decide which accounts will be subject to further intrusions."[105] When there is "unbridled discretion" given to the government or even just a lack of an "objective measure that limits the [government's] discretion in obtaining information as to each cellular telephone in the geofence," courts have often held that the warrants lack the necessary particularity.[106]

3. Potential to Obtain Data from Innocent Individuals

Another concern about geofence warrants is their ability "to capture vast swaths of location data of individuals not connected to the crime."[107] When the warrant is sufficiently limited both geographically and temporally to minimize the amount of data collected on innocent individuals, courts are more likely to find the warrant constitutional.[108] For example, in *Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, arson crimes "occurred in the early hours of the morning when commercial businesses are usually closed and unoccupied," so the times requested in the geofence warrant were in the "wee hours of the morning" when streets are "generally sparsely populated by pedestrians" and drivers.[109] The court found that the warrant was not overbroad because the limitations ensured there was probable cause that the location data of the potential suspects and witnesses was collected by Google and that the warrant would not "result in the collection of a broad sweep of data from uninvolved individuals for which there is no probable cause."[110]

---

104. *Id.* at *6.

105. United States v. Chatrie, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022).

106. *In re* Search of Information Stored at Premises Controlled by Google, as further described in Attachment A, No. 20 M 297, 2020 WL 5491763, at *6 (N.D. Ill. July 8, 2020); United States v. Wright, No. CR419-149, 2023 WL 6566521, at *22 (S.D. Ga. May 25, 2023).

107. *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 358 (N.D. Ill. 2020); *Search of Info. Stored at Premises Controlled by Google*, 2023 WL 2236493, at *14 (granting the warrant request because there was probable cause and particularity, and the request was "not overbroad, because its proposed geographic area and time periods closely track the probable cause to justify the requested disclosure of information, and because it minimizes the likelihood that the Step One warrant will sweep up personally identifiable data of uninvolved persons").

108. *See Search Info. Stored at Premises Controlled by Google*, 2023 WL 2236493, at *13 (weighing the interest of uninvolved third parties against the interest of identifying suspects but finding the third-party interest did not render the warrant overbroad in part because "[r]easonable investigation '[could not] produce a more particular description' of the place to be searched").

109. *Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d at 358.

110. *Id.* at 357–59.

In contrast, courts have denied warrants when the geographic area or time frame is so large that particularized probable cause was lacking as to each Google user within the geofence.[111] For example, in *Search of Information Stored at Premises Controlled by Google*, the District Court for the Northern District of Illinois found that the warrant lacked individualized probable cause because it sought information on device users simply because of their "'propinquity' to the crime scenes or to the Unknown Subject."[112]

III. THREE POTENTIAL CONCLUSIONS ON GEOFENCE WARRANTS: ALWAYS, NEVER, OR SOMETIMES ALLOW THEM

When geofence warrant cases reached the federal circuit courts, the courts began analyzing the location data requested in a geofence warrant under a reasonable expectation of privacy test to determine whether a search occurred.[113] While some district courts had mentioned the reasonable expectation of privacy test in prior years, none had reached a conclusion as to whether using this location data constituted a search.[114] The Fourth Circuit originally found that there was no reasonable expectation of privacy in the location data used in geofences, but it took less than a month before the Fifth Circuit disagreed and created a circuit split.[115] The courts split on two main issues: (1) whether users have a reasonable expectation of

111. *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 752–53 (N.D. Ill. 2020); *see* United States v. Chatrie, 590 F. Supp. 3d 901, 925–27 (E.D. Va. 2022) (finding that the "warrant lacked any semblance of such particularized probable cause," partly due to the fact that the geofence had a 150-meter radius in an urban environment—70,686 square meters of land "located in a busy part of the Richmond metro area"); United States v. Brown, No. 1:16-CR-427-AT-JKL-31, 2025 WL 1674283, at *16–17 (N.D. Ga. June 13, 2025) (finding "a person's mere propinquity to a crime scene is not alone probable cause to suspect him of a crime").

112. *Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 752–53.

113. Because geofence warrants are reverse warrants that are used to identify suspects based on their locations, it was only a matter of time before the reasonable expectation of privacy test would be applied. Berris & Wild, *supra* note 51; *see* United States v. Chatrie, 107 F.4th 319, 325 (4th Cir. 2024); United States v. Smith, 110 F.4th 817, 836 (5th Cir. 2024).

114. *Chatrie*, 590 F. Supp. 3d at 926 ("As this Court sees it, analysis of geofences does not fit neatly within the Supreme Court's existing 'reasonable expectation of privacy' doctrine as it relates to technology. That run of cases primarily deals with *deep*, but perhaps not *wide*, intrusions into privacy."); United States v. Rhine, 652 F. Supp. 3d 38, 82 (D.D.C. 2023) ("While the Court does not decide the question of whether Defendant had a reasonable expectation of privacy over his [Location History] data, it bears in mind the principles reflected in the Supreme Court's recent opinions as it turns to evaluate the sufficiency of the Geofence Warrant.").

115. While the Eleventh Circuit heard a case on geofences and appeared to agree with the Fourth Circuit, it involved data obtained from a third party, so it is factually distinguishable and will not be discussed. *See* United States v. Davis, 109 F.4th 1320, 1329 (11th Cir. 2024) ("Even if a person has a privacy interest in the data on his own phone, he does not have that interest in the data on someone else's phone. Because the geofence revealed the location of an open program that was not Davis's and was not on a phone in his exclusive possession or control, he cannot argue that he had a privacy interest in this data that gives him Fourth Amendment standing to challenge the search.").

privacy in geofence location data, and (2) whether geofence warrants can be constitutional.[116]

There are three conclusions a court could reach when analyzing reverse warrants such as geofence warrants: (1) align with the Fourth Circuit's original opinion and find that warrants are never required, giving law enforcement sole discretion to decide what and how much data they collect; (2) follow the Fifth Circuit's reasoning and find that reverse warrants are never allowed; or (3) allow the warrant when the warrant application details a filter that will sufficiently limit the scope of the search.[117]

Categories of Decisions on Reverse Warrant Cases		
Never Required	Never Allowed	Allowed with a Filter
Chatrie in the Fourth Circuit's original decision	*Smith* in the Fifth Circuit	*Seymour* in the Colorado Supreme Court; *Jones* in the Georgia Supreme Court

A. Geofence Warrants Never Required

The first case on geofences heard by a federal appellate court—*United States v. Chatrie*—resulted in a determination that there is no reasonable expectation of privacy in geofence location data and no warrant is required to obtain it.[118] Following a credit union robbery in Virginia, a detective investigated and obtained a geofence warrant since the suspect was seen on security cameras carrying a cell phone during the robbery.[119] In response to the warrant, Google followed its three-step procedure and provided 209 location data points from 19 devices that appeared within the geofence during the specified hour-long time period at Step One.[120] The detective narrowed down his search to 9 devices and requested Step Two information from them, which resulted in 680 location data points over a two-hour time period.[121] At Step Three, the detective requested identifying information for 3 accounts—one of which belonged to Okello Chatrie, who was subsequently indicted.[122]

After the district court denied Chatrie's motion to suppress the evidence from the geofence warrant and the case went to the Fourth Circuit, the court originally determined that Chatrie had no reasonable expectation of privacy in his two hours' worth of geofence location data—data that amounted to no more than an

116. *Chatrie*, 107 F.4th at 330–31; *Smith*, 110 F.4th at 834–35.

117. *See* Kerr, *supra* note 12, at 18–22.

118. *Chatrie*, 107 F.4th at 325, 330–34. As mentioned above, the Fourth Circuit reheard this case en banc and issued a new, one-line decision in April 2025, but the analysis provided by the original opinion is discussed here, as it is representative of one category of potential decisions that courts might reach in the context of reverse warrants.

119. *Chatrie*, 590 F. Supp. 3d at 937; *Chatrie*, 107 F.4th at 324.

120. *Chatrie*, 107 F.4th at 325.

121. *Id.*

122. *Id.*

"individual trip viewed in isolation."[123] After discussing some location tracking and third-party doctrine cases,[124] the court distinguished the facts from those in *Carpenter* and focused on two rationales: "[T]he limited degree to which the information sought implicates privacy concerns and the voluntary exposure of that information to third parties."[125] Because Chatrie knowingly and voluntarily exposed his location data to Google by opting into the Location History service, the court found that the information obtained was "voluntarily conveyed to anyone who wanted to look" and was "no more revealing than [one's] bank records or telephone call logs."[126] Ultimately, the court held that the government did not conduct a search since the third-party doctrine applied.[127] Thus, the court impliedly found that no warrant was required in order to obtain geofence location data.[128]

B. Reverse Warrants Never Allowed

Less than a month after the original *Chatrie* decision, the Fifth Circuit decided *United States v. Smith*, which concluded that individuals have a reasonable expectation of privacy in geofence data and that geofence warrants are categorically unconstitutional.[129] After mail bags containing over $60,000 were stolen, postal inspectors investigated and obtained a geofence warrant to locate potential suspects and witnesses.[130] The issued warrant laid out a procedure similar to Google's three-step process but required additional legal process for "any additional information" after Step One.[131] The warrant also limited the search location to 98,192 square meters in a one-hour timeframe on the date of the robbery, but Google conducted a much broader search and produced data from an area around 378,000 square meters.[132] After receiving the Step One data, neither postal inspector applied for another warrant.[133] Instead, they asked Google for information at Steps Two and Three for *all* devices produced at Step One—leading to the indictment of Jamarr Smith and Gilbert McThunel.[134]

After the district court allowed evidence from the geofence warrant, the defendants appealed, and the Fifth Circuit determined that individuals have a reasonable expectation of privacy in geofence data and that geofence warrants are unconstitutional general warrants.[135] The court noted that many of the concerns present in *Carpenter* were present in the context of geofence warrants, and the most troubling was the "potential for 'permeating police surveillance.'"[136] Even when

---

123. *Id.* at 325, 330.
124. *See supra* Section II.B.
125. *Chatrie*, 107 F.4th at 330.
126. *Id.* at 330–31.
127. *Id.* at 332, 339.
128. *See id.* at 332, 334 (noting that a warrant is required only when someone's reasonable expectation of privacy is invaded).
129. 110 F.4th 817, 820–21 (5th Cir. 2024).
130. *Id.* at 821.
131. *Id.* at 826, 838.
132. *Id.* at 827.
133. *Id.* at 828.
134. *Id.* at 828–29.
135. *Id.* at 829–30, 836, 838.
136. *Id.* at 832–33 (quoting Carpenter v. United States, 585 U.S. 296, 305 (2018)).

only a "snapshot of precise location data" is obtained, the court emphasized that this can still be highly intrusive and can expose individuals' locations when they are in "some of the most private and intimate" places, such as their residences.[137] Additionally, the court questioned whether "electronic opt-in processes" are truly informed and voluntary.[138]

As for the constitutionality of the geofence warrants, the court explained that geofence warrants "present the exact sort of 'general, exploratory rummaging' that the Fourth Amendment was designed to prevent."[139] While the results of a geofence warrant might be narrowly tailored, the search itself cannot be.[140] Instead, Google must search its entire database of 592 million accounts for all locations at a given time, and the warrants never include a specific user but rather merely identify a time period and geographic area where "any given user *may* turn up post-search."[141] Because of this, the court held that geofence warrants are general warrants categorically prohibited by the Fourth Amendment.[142]

C. Reverse Warrants Allowed with a Sufficient Filter

While not part of the federal circuit divide, two state courts have produced decisions that are representative of a position that falls between those of the Fourth and Fifth Circuits.[143] Specifically, these two cases suggest using an approach focused on the filter applied to the data ultimately provided to law enforcement.[144] In *People v. Seymour*, the Colorado Supreme Court ruled that a reverse keyword search warrant was reasonable even though Google had to search through its *entire* database to find a responsive hit.[145] After law enforcement had "exhausted all their leads without identifying a single suspect" in a suspected residential arson, they sought a reverse keyword warrant to obtain an anonymized list of any Google accounts that had searched the address in the 15 days before the fire.[146] The Court ultimately found that the "scope of the place to be searched" was reasonable and sufficiently limited due to the "filter provided by the search parameters set forth in the warrant."[147] Even though the government, "in some lightning-fast, digital sense,

---

137. *Id.* at 833.

138. *Id.* at 835. Using an example to demonstrate its point, the court reiterated the example from the *Chatrie* district court decision and stated that "a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting 'YES, I'M IN' at midnight while setting up Google Assistant, even if some text offered warning along the way." *Id.* at 836.

139. *Id.* at 837 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)).

140. *Id.* at 837–38.

141. *Id.* at 836–37.

142. *Id.* at 838.

143. *See generally* People v. Seymour, 536 P.3d 1260 (Colo. 2023) (analyzing the filter used in a reverse keyword search context); Jones v. State, 913 S.E.2d 700 (Ga. 2025) (utilizing a filter approach in the geofence context).

144. Kerr, *supra* note 12, at 22–25.

145. *Seymour*, 536 P.3d at 1276, 1280.

146. *Id.* at 1268–70.

147. *Id.* at 1267, 1275–76, 1278 ("Although the database is large, the narrow search terms, the timeframe constraints, and the fact that the initial search was anonymized all served to minimize any invasion of privacy resulting from the search.").

very cursorily examine[d] unrelated documents," this did not make the search unconstitutional because "the narrow search terms, the timeframe constraints, and the fact that the initial search was anonymized all served to minimize any invasion of privacy resulting from the search."[148]

Similarly, in *Jones v. State*, the Supreme Court of Georgia utilized a filter-focused approach and concluded that a geofence warrant satisfied the probable cause and particularity requirements.[149] After a woman was found dead in her home under suspicious circumstances, the government sought a geofence warrant from Google to determine what devices were within 100 meters of the home during a four-hour period on the night of the murder.[150] Upon review of the data, the police found a device to be "very suspicious" because it was near the home around the time of the murder and was "moving around the side of the home where the suspect was seen in the surveillance video."[151] Even though "Google's initial search for the requested information would 'touch' the data of *all* Google users,"[152] the Court explained that investigators do not view all of the data in the system, so the "privacy of the information that is not surfaced by the search query is preserved from the investigator."[153] Instead, "when an investigator runs . . . a search [on a database], he types a set of search terms or criteria into a search box, and then he sees the results, if any, that the query returns."[154] Thus, the Court concluded that it was "hard to see how one could call what the investigator did a Fourth Amendment 'search' of the information in the database that was not returned as a search result."[155]

IV. REASONABLE EXPECTATION OF PRIVACY IN GEOFENCE LOCATION DATA

The Fourth and Fifth Circuits disagreed over whether there is a reasonable expectation of privacy in geofence data, with the Fourth Circuit originally finding no reasonable expectation of privacy and the Fifth Circuit finding otherwise.[156] Since *Carpenter* is the only case from the Supreme Court offering guidance on how to analyze the reasonable expectation of privacy in the context of digital data,[157] lower courts must try to use the factors described in the opinion.[158] One survey of

148. *Id.* at 1276; *see also In re* Geo-Fence & Cell Site Location Info. Search Warrants, No. CM22000505-01, 2022 WL 22916777, at *1, *3 (Va. Cir. Ct. July 28, 2022) (finding that a warrant based on a particular search term was constitutionally permissible because the "search term was a specific, unique, not-easily confused search term entered during an unusual time of the day and for a limited period that would, more probably than not, be related to the specific crime under investigation").

149. Jones v. State, 913 S.E.2d 700, 703–04 (Ga. 2025).

150. *Id.*

151. *Id.* at 704.

152. *Id.* at 708.

153. *Id.*

154. *Id.*

155. *Id.*

156. United States v. Chatrie, 107 F.4th 319, 330–31 (4th Cir. 2024); United States v. Smith, 110 F.4th 817, 834–35 (5th Cir. 2024).

157. *See* Carpenter v. United States, 585 U.S. 296, 320 (2018).

158. *See generally Chatrie*, 107 F.4th 319 (applying *Carpenter* to geofence warrants); *Smith*, 110 F.4th 817 (same).

cases discussing *Carpenter* substantively through mid-2021 revealed that courts focused on the amount of data collected, the voluntary nature of the disclosure, and the revealing nature of the data.[159] In the over 180 cases that have mentioned *Carpenter* substantively between mid-2021 and mid-2025,[160] the focus on those factors has remained.

Court	Quantity of Data Collection[161]	Voluntariness[162]	Revealing Nature[163]

159. Tokson, *Aftermath of* Carpenter, *supra* note 89, at 1823; *see* Matthew Tokson, *The* Carpenter *Test as a Transformation of Fourth Amendment Law*, 2023 U. ILL. L. REV. 507, 518 [hereinafter Tokson, *The* Carpenter *Test*].

160. As part of writing this Note, I conducted a survey of over 180 cases from mid-2021 through mid-2025 that Westlaw indicated had substantively discussed the *Carpenter* decision, and I noted which factors were mentioned by the courts in the various decisions. Most of the cases were decided on procedural grounds, the good faith exception, or an exigency exception, so there were only a limited number of cases that analyzed the *Carpenter* factors.

161. *See, e.g.*, United States v. Salaman, 742 F. Supp. 3d 221, 226, 231 (D. Conn. 2024) (finding, in light of *Carpenter*, that nearly three months of continuous surveillance outside a person's home was "prolonged and targeted video surveillance" that required a warrant); United States v. Pobre, No. 8:19-CR-348-PX, 2022 WL 1136891, at *5 (D. Md. Apr. 15, 2022) (finding that *Carpenter* did not apply in part because the software at issue did not "amass a 'trail of location data'" but rather only disclosed a single data point—the IP address of a user node); Commonwealth v. Pacheco, 263 A.3d 626, 640–41 (Pa. 2021) (finding that the acquisition of 108 days of real-time CSLI implicated the same concerns present in *Carpenter* as this much data resulted in "near perfect surveillance of his location over the course of a lengthy criminal investigation").

162. *See, e.g.*, Sanchez v. Los Angeles Dep't of Transp., 39 F.4th 548, 559 (9th Cir. 2022) (finding that the considerations in *Carpenter* were not present here in part because the defendant voluntarily conveyed his location to the operator "in the ordinary course of business" when using an electric scooter); United States v. Bledsoe, 630 F. Supp. 3d 1, 13 (D.D.C. 2022) (distinguishing *Carpenter* because the "only way that Facebook was able to determine when and where a user engaged in account activity on January 6, 2021, is by virtue of the user making an affirmative and voluntary choice" to download Facebook, create an account, and "take no available steps to avoid disclosing his location"); Commonwealth v. Reed, 647 S.W.3d 237, 247–48 (Ky. 2022) (finding *Carpenter* compelling in part because the real-time CSLI was "involuntar[ily] convey[ed]" to the cell-service providers "without a cellphone owner's knowledge or consent").

163. *See, e.g.*, United States v. Baker, 563 F. Supp. 3d 361, 381 (M.D. Pa. 2021) (noting "the discovery of one's presence inside a private home" can "provide an intrusive glimpse into his private affairs"); United States v. Manning, No.1:19-CR-00376-TWT-RGV, 2021 WL 5236660, at *6 (N.D. Ga. Aug. 20, 2021) (finding the information revealed by a tower dump distinct from *Carpenter* because the defendant did not show "that it tracks a person's movements from a public thoroughfare 'into private residences, doctor's offices, political headquarters, and other potentially revealing locales'" (quoting Carpenter v. United States, 585 U.S. 296, 311 (2018)); Commonwealth v. Perry, 184 N.E.3d 745, 759, 762 (Mass. 2022) (noting that courts "have considered the extent to which the surveillance, even if less comprehensive, tended to reveal highly intimate or personal details" and finding that the tower dump at issue produced "highly personal and private" information, in part because it could provide identifying information in private and public settings).

Federal	39	21	51
Overall	59	39	78

In applying these factors to the geofence cases, the Fourth and Fifth Circuits disagreed on two main *Carpenter* rationales: (1) how limited or invasive a snapshot of location information is and (2) whether users knowingly and voluntarily opt in.[164] The Fourth Circuit originally concluded that there is no reasonable expectation of privacy in geofence data because it is not highly invasive and users voluntarily opt in to the Location History service.[165] In contrast, the Fifth Circuit concluded that individuals do have a reasonable expectation of privacy in their geofence data, in part because the data is highly invasive and the opt-in process is not truly voluntary.[166] This Part argues that instead of following the Fourth Circuit's original analysis, courts should recognize a reasonable expectation of privacy in geofence data since it exposes large quantities of revealing data and has the capability to expose information from inside individuals' constitutionally protected areas.

A. Large Quantities of Highly Invasive Data

The Fourth Circuit originally found the geofence location data to be limited in nature, while the Fifth Circuit found it to be invasive.[167] This difference might be the result of the additional precedent in the Fourth Circuit relating to location-tracking technology.[168] In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, community advocates challenged the City of Baltimore's aerial-surveillance program, which involved planes equipped with a camera technology that captured 32 square miles per image per second and flew at least 40 hours per week.[169] The Fourth Circuit interpreted *Carpenter* to "solidif[y] the line between short-term tracking of public movements" and "prolonged tracking that can reveal intimate details through habits and patterns."[170] As a result, the court concluded that Baltimore's program violated individuals' reasonable expectation of privacy because it provided the government with retrospective "detailed, encyclopedic" records of everyone in the city over a month and a half.[171] The court emphasized that because of the quantity of data in question, it enabled revealing "deductions about 'what a person does repeatedly, what he does not do, and what he does

164. United States v. Chatrie, 107 F.4th 319, 330–31 (4th Cir. 2024); United States v. Smith, 110 F.4th 817, 834–35 (5th Cir. 2024).

165. *Chatrie*, 107 F.4th at 330–32.

166. *Smith*, 110 F.4th at 834–36.

167. *Chatrie*, 107 F.4th at 330–31; *Smith*, 110 F.4th at 834.

168. Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 334 (4th Cir. 2021); *Chatrie*, 107 F.4th at 334.

169. 2 F.4th at 333–34.

170. *Id.* at 341; Carpenter v. United States, 585 U.S. 296, 315 (2018) (distinguishing between a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years" and a "person's movement at a particular time").

171. *Beautiful Struggle*, 2 F.4th at 341.

ensemble,' which 'reveal[s] more about a person than does any individual trip viewed in isolation.'"[172]

With this background and focus on a distinction between "individual trips" and prolonged tracking,[173] the Fourth Circuit could easily distinguish the 2 hours of geofence location data in *Chatrie* from the 45 days' worth of data collected in 12-hour increments in *Beautiful Struggle*.[174] In *Chatrie*, the court called the two hours of geofence data an "individual trip viewed in isolation" that was "far less revealing" than data obtained in *Carpenter* and instead was comparable to the short-term tracking of public movements in *Knotts*.[175] There is obviously a stark contrast between the length of the data collection involved in *Chatrie* and *Beautiful Struggle*, but in focusing primarily on the length of the data collection and how the data must allow deductions about *repeated* activities, the court in *Chatrie* ignored the quantity of data provided by the geofence technology and the precision of the data.[176] In fact, the police collected about 76 data points on each person surveilled in *just two hours* with the geofence technology—compared to the 101 data points collected in *Carpenter* over the course of *a full day*.[177] Even though the durations of the data collection were vastly different in *Carpenter* and *Chatrie*, the data quantities in question were very similar. Additionally, each geofence data point could "hunt down" a user's location within meters, including "locating the specific *floor in a building* where a person might be"—compared with the CSLI data in *Carpenter* that placed a defendant in a section ranging from "a dozen" to "several hundred" city blocks.[178] Not only does this data create a "digital dossier" that can "unveil a person's anonymous speech and personal associations," but it is "even more 'detailed, encyclopedic, and effortlessly compiled' than CSLI."[179] Yet the Fourth Circuit ignored this entirely by focusing solely on the length of the data collection.[180] In contrast, in *Smith*, the Fifth Circuit noted the similarities with the CSLI data in *Carpenter* and emphasized the intrusiveness of "even a snapshot of precise location data."[181] The Fifth Circuit's analysis seems more appropriate given the potential intrusiveness of geofence data, and this intrusiveness weighs in favor of finding that individuals have a reasonable expectation of privacy in their geofence location data.

B. Potential to Intrude on Constitutionally Protected Areas

While the quantity of data collected is one major factor that courts look at in determining whether there is a reasonable expectation of privacy in the collection

---

172. *Id.* at 342 (quoting United States v. Maynard, 615 F.3d 544, 562–63 (D.C. Cir. 2010)).

173. *Id.*

174. United States v. Chatrie, 107 F.4th 319, 329–30 (4th Cir. 2024); *Beautiful Struggle*, 2 F.4th at 341–42.

175. *Chatrie*, 107 F.4th at 330–31.

176. *Id.* at 349 (Wynn, J., dissenting).

177. *Id.*

178. *Id.*

179. Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002); *Chatrie*, 107 F.4th at 330–31, 349 (Wynn, J., dissenting).

180. *Chatrie*, 107 F.4th at 349 (Wynn, J., dissenting).

181. United States v. Smith, 110 F.4th 817, 833 (5th Cir. 2024).

of digital data under *Carpenter*, courts have also consistently expressed concerns about the places and associations that might be revealed with location tracking.[182] Individuals have a reasonable expectation of privacy in constitutionally protected areas such as their homes, and geofence warrants can collect data on innocent individuals while they are in their homes.[183] The Fourth Circuit did not even address this concern because it concluded that Chatrie lacked Fourth Amendment standing to raise the argument that geofences have the potential to reveal information "that could not otherwise have been obtained without physical intrusion into a constitutionally protected area."[184] Because he did not "allege that the Location History data obtained by the government invaded his constitutionally protected space,"[185] the Fourth Circuit decided to save the issue for a different case.

But Judge Wynn dissented in the Fourth Circuit's 2024 decision and cited two Supreme Court opinions that strongly supported his position.[186] First, Judge Wynn noted that in *Kyllo v. United States*, the Supreme Court rejected the argument that the Fourth Amendment is only implicated if a search using sense-enhancing technology catches intimate information inside a constitutionally protected area.[187] Instead, a search occurs even when there is a *potential* to collect intimate details from constitutionally protected areas.[188] Second, Judge Wynn pointed out that no facts in *Carpenter* showed that the CSLI data collection occurred

182. *See, e.g.*, United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (expressing concerns that the location tracking could reveal a "wealth of detail about her familial, political, professional, religious, and sexual associations" since the location data can disclose "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on" (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009))); United States v. Baker, 563 F. Supp. 3d 361, 381 (M.D. Pa. 2021) ("Although perhaps not as invasive as the comprehensive data collected in *Carpenter*, the discovery of one's presence inside a private home [through a location data ping] does reveal 'intricacies of private life.' Personal associations, for instance, often take place within the walls of private dwellings, so even a snapshot of location information, reaching the target beyond the threshold of these walls, can provide an intrusive glimpse into his private affairs."); *In re* Four Applications for Search Warrants Seeking Info. Associated with Particular Cellular Towers, No. 3:25-CR-38-CWR-ASH, 2025 WL 603000, at *6 (S.D. Miss. Feb. 21, 2025) (finding a search occurred in part because the tower dump could collect information from "residential neighborhoods, a mall, medical clinics, schools, shopping centers, a supermarket, churches, a courthouse, hotels, interstate highways, a train station, and an airport").

183. *See* Florida v. Jardines, 569 U.S. 1, 11 (2013).

184. United States v. Chatrie, 107 F.4th 319, 350 (4th Cir. 2024) (Wynn, J., dissenting) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

185. *Id.* at 336–37 (majority opinion).

186. *Id.* at 351–52 (Wynn, J., dissenting).

187. *Id.* at 351. In *Kyllo v. United States*, law enforcement used a thermal imager, a sense enhancing device, to determine if the amount of heat emanating from Kyllo's home was consistent with heat lamps used for growing marijuana. 533 U.S. 27, 29–30 (2001). The Court held that a search occurs when police obtain any information from the home's interior via sense-enhancing technology that they could not otherwise obtain "without physical 'intrusion into a constitutionally protected area.'" *Id.* at 34–45 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

188. *See Chatrie*, 107 F.4th at 351 (Wynn, J., dissenting).

in any of the defendant's protected spaces.[189] The Supreme Court, instead, focused on the "*capabilities* during the intrusion as opposed to the specific facts of each intrusion" to conclude that Carpenter had a reasonable expectation of privacy in that data and thus had standing.[190] "[A]ll citizens would reasonably expect privacy in data that continuously and retrospectively tracked their movements in [non-public] protected spaces with remarkable precision."[191] Therefore, because geofence location data has the capability of doing this, Chatrie would have a reasonable expectation of privacy from the intrusions of this geofence—a technology that "could capture a church and residences at Step One and was boundless at Step Two."[192]

Similarly, the Fifth Circuit reasoned that the reasonable expectation of privacy analysis in *Carpenter* did not rely on whether the data collection actually occurred in spaces granted Fourth Amendment protection.[193] Instead, the question was whether the technology used by law enforcement "had the *capability* of providing data that offered 'an all-encompassing record of [a person's] whereabouts.'"[194] Here, the Location History data produced in response to geofence warrants has that capability because it can provide detailed and retrospective Location History data for anyone who has the service enabled, regardless of whether "a particular individual is suspicious or moving within an area that is typically granted Fourth Amendment protection."[195]

Moreover, the dissent and the Fifth Circuit have a stronger basis in precedent on the issue of standing, and the Fourth Circuit majority should not have disposed of this argument so quickly.[196] Instead, the Fourth Circuit should have reconciled the differences between geofence data and what it claimed was the highly comparable short-term tracking of *public* movements in *Knotts*.[197] Unlike a GPS tracker used on public roads that you can turn off when it enters a constitutionally protected area, there is not a way to tailor a geofence narrowly enough to ensure that it does not invade constitutionally protected areas such as homes.[198] Thus, this fact seems to lean in favor of finding that individuals have a reasonable expectation of privacy in their geofence location data.[199]

C. The "Voluntariness" of the Electronic Opt-In Process

Further, the Fourth and Fifth Circuits viewed the electronic opt-in process differently.[200] The Fourth Circuit originally emphasized that users must take an

---

189. *Id.*
190. *Id.*
191. *Id.*
192. *Id.*
193. United States v. Smith, 110 F.4th 817, 834 n.8 (5th Cir. 2024).
194. *Id.* (quoting Carpenter v. United States, 585 U.S. 296, 311 (2018)).
195. *Id.* at 834.
196. *See id.* at 831 n.5.
197. United States v. Chatrie, 107 F.4th 319, 330–31 (4th Cir. 2024).
198. *See Smith*, 110 F.4th at 837–38 ("While the *results* of a geofence warrant may be narrowly tailored, the *search* itself is not."); Florida v. Jardines, 569 U.S. 1, 10–11 (2013).
199. *Smith*, 110 F.4th at 834.
200. *Chatrie*, 107 F.4th at 330; *Smith*, 110 F.4th at 835.

affirmative action and thus knowingly and voluntarily convey their information to Google, while the Fifth Circuit explained that electronic opt-in processes are "hardly informed" and often not voluntary.[201] On this issue, the Fourth Circuit's analysis is likely more in line with *Carpenter*. In *Carpenter*, the Supreme Court explicitly noted that CSLI did not require "any affirmative act on the user's part."[202] In contrast, in the context of Google's Location History, users must take an affirmative action to allow Google to track their location.[203] Further, in *Carpenter*, the Court noted that users did not voluntarily expose their information in part because "cell phones and the services they provide are 'such a pervasive and insistent part of daily life.'"[204] While cell phones might be "indispensable to participation in modern society," using Google's Location History service is not.[205] In fact, "two-thirds of active Google users have not enabled Location History," so this is strong evidence that the Location History service is not required for modern life.[206]

In addition, *Carpenter* did not overrule existing Fourth Amendment precedent that has not required users to be aware of the full extent to which their data might be used.[207] In fact, the Supreme Court has consistently found that the Fourth Amendment does not prohibit obtaining information revealed to a third party and conveyed to the government even if the information is revealed by the individual "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[208] Applying this to the geofence context, even if users assume that Google will only use their location data for the limited purpose of giving map directions or tracking a bike ride, that assumption cannot protect their data when they voluntarily give it for that other purpose. Further, even if the electronic opt-in process is "hardly informed" as the Fifth Circuit claims, as long as users convey their data anyway, that action is likely sufficient to meet the voluntary exposure standard.[209]

D. Summary of Points

While there are strengths and weaknesses to each court's analysis, other courts should recognize a reasonable expectation of privacy in geofence location data and enforce a warrant requirement. An analysis of the key *Carpenter* factors—(1) the amount of data collected, (2) the revealing nature of the data collected, and

---

201. *Chatrie*, 107 F.4th at 330; *Smith*, 110 F.4th at 835.

202. Carpenter v. United States, 585 U.S. 296, 298 (2018).

203. *Chatrie*, 107 F.4th at 322–23, 331.

204. *Carpenter*, 585 U.S. at 298 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

205. *Id.*; ORIN KERR, THE DIGITAL FOURTH AMENDMENT: PRIVACY AND POLICING IN OUR ONLINE WORLD 168 (2025).

206. *Chatrie*, 107 F.4th at 331.

207. *Carpenter*, 585 U.S. at 298; United States v. Miller, 425 U.S. 435, 443 (1976).

208. *Miller*, 425 U.S. at 443; *see* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 108–09 (2011) (noting that even if a third party promises or contracts with a user to protect his data from the government, the Supreme Court would find this insufficient to provide a reasonable expectation of privacy in that data).

209. United States v. Smith, 110 F.4th 817, 835 (5th Cir. 2024).

(3) the voluntary nature of the disclosure—weigh in favor of this conclusion.[210] Specifically, the Location History service can collect a large quantity of data in a short period of time since it can track a user's location in precise detail every two minutes.[211] Additionally, geofence data can be extremely invasive, especially when considering the potential for collecting intimate information from constitutionally protected areas.[212] While the electronic opt-in process might be considered voluntary, the other factors, and therefore the key *Carpenter* factors on balance, weigh in favor of recognizing a reasonable expectation of privacy. Thus, courts should recognize a reasonable expectation of privacy in geofence location data and enforce a warrant requirement.

V. PROPERLY CONSTRAINED REVERSE WARRANTS AND GENERAL WARRANTS

The Fourth and Fifth Circuits' opinions on geofence warrants constitute two ends of the spectrum, with the Fourth Circuit's original decision on one extreme, determining that warrants are never required for geofence location data, and the Fifth Circuit decision on the other, concluding that geofence warrants are categorically unconstitutional because they are general warrants.[213] Specifically, the Fifth Circuit took issue with Step One of the warrant response process, as it does not limit the search and instead requires Google to "search through its *entire* database" of 592 million accounts for "*all* of [its users'] locations at a given point in time" while law enforcement has "*no idea* who they are looking for, or whether the search will even turn up a result."[214] This Part argues that instead of following the Fifth Circuit's reasoning, courts should allow geofence warrants and not deem them categorically unconstitutional.

A. Conflicts with Precedent

First, the Fifth Circuit's conclusion seems to conflict with Supreme Court precedent. For example, in *United States v. Karo*—a case that involved a GPS location tracker—the Court provided an explanation for how to draft a warrant that would meet the particularity requirement in cases where the government does not know the exact place to be searched.[215] Specifically, the Court noted that the government could "describe the object into which the [tracker] is to be placed, the circumstances that led agents to wish to install the [tracker], and the length of time for which [tracker] surveillance is requested."[216] Similar to the police who did not know the place to be searched in *Karo*, police applying for geofence warrants do not

---

210. Tokson, *Aftermath of* Carpenter, *supra* note 89, at 1823; *see* Tokson, *The* Carpenter *Test*, *supra* note 159, at 510 (listing the three factors).

211. *Chatrie*, 107 F.4th at 349 (Wynn, J., dissenting).

212. *Smith*, 110 F.4th at 834.

213. *Chatrie*, 107 F.4th at 336; *Smith*, 110 F.4th at 836, 838. General warrants merely specify an offense and give law enforcement the discretion to decide "which persons should be arrested and which places should be searched." Steagald v. United States, 451 U.S. 204, 220 (1981).

214. *Smith*, 110 F.4th at 837.

215. 468 U.S. 705, 718 (1984).

216. *Id.*

know the person for whom they are searching.[217] But instead of saying that no warrant can be sufficiently particular, it is more in line with *Karo* to allow the warrant and simply describe the "database into which the query is made, combined with the length of time (and amount of geographic space) the warrant covers."[218] While there are obvious differences between location trackers like those in *Karo* and geofences, in both cases, one can draft a warrant supported by particularized probable cause by describing what will be searched, how it will be searched, and how long the tracking will last.[219]

Additionally, the Fifth Circuit's concern about the size of the database to be searched seems hard to square with *Carpenter*.[220] In *Carpenter*, the Supreme Court determined that warrants were sufficient for CSLI data, which will generally be in large databases.[221] If the Fifth Circuit bases its constitutional determination on not just the type of data but also the size of the database, this would add an additional restriction and seemingly conflict with the broader *Carpenter* ruling.[222]

Further, while not Supreme Court precedent, *People v. Seymour* analyzed a reverse warrant that required a search through a large database,[223] and this decision is also at odds with the Fifth Circuit's reasoning and distinction based on the size of a database. In *Seymour*, the Colorado Supreme Court ruled that a reverse keyword search warrant was reasonable even though Google had to search through its *entire* large database to find a responsive hit.[224] The Court ultimately found that the scope of the place to be searched was sufficiently limited by the filter provided by the

---

217. *Id.*

218. Kerr, *supra* note 14.

219. *See* Orin S. Kerr, *The ACLU's Response to My Post on the Fifth Circuit's* Smith *Ruling—And My Reply to the ACLU*, VOLOKH CONSPIRACY (Aug. 16, 2024, at 04:30 MT), https://reason.com/volokh/2024/08/16/the-aclus-response-to-my-post-on-the-fifth-circuits-smith-ruling-and-my-reply-to-the-aclu/ [https://perma.cc/8LXW-RHQH]. For example, a beeper is a physical item that is installed and will only track a limited number of people, but a geofence can track a large number of people into any range of places and collect extensive information. *Id.* In addition, the police in *Karo* knew significantly more information than "what the object is, why it is relevant to the crime under investigation, who is likely to take possession of it, and for what criminal purpose." *Id.* In contrast, the police do not know many details, if any, about whom they are searching for when they ask for information via a geofence. *Id.*

220. United States v. Smith, 110 F.4th 817, 837 (5th Cir. 2024).

221. Kerr, *supra* note 14.

222. *Id.*; *see also* Jones v. State, 913 S.E.2d 700, 708 (Ga. 2025) (rejecting an argument that geofence warrants are overbroad because they require Google to search its database and "effectively 'look[] at' every Google account in the world," and instead finding that "[d]atabase searches are a routine part of criminal investigations"); United States v. Brown, No. 1:16-CR-427-AT-JKL-31, 2025 WL 1674283, at *14 (N.D. Ga. June 13, 2025) (reasoning that the geofence warrant was not a general warrant because, even though Google's "internal processes require[d] that it start with all user information within its database before producing the information specified in the warrant, it [did] not follow that the Government conducted a search of the whole of the database").

223. People v. Seymour, 536 P.3d 1260, 1276, 1280 (Colo. 2023).

224. *Id.*; *see supra* Section III.C.

warrant's search parameters—nine specified keywords.[225] The Colorado Supreme Court's reasoning would help further law enforcement efforts by allowing them to search any digital database if there are reasonable parameters that limit their discretion, while the Fifth Circuit's reasoning would hinder law enforcement efforts whenever a court deems a database too large.

Additionally, the relevant question for Fourth Amendment purposes as described in *Rhine* is "not *how* Google runs searches on its data, but *what* the warrant authorizes the Government to search and seize."[226] When law enforcement asks a third party for data, such as CSLI or geofence location data, this necessarily requires the third party to "search some group of records larger than those specifically requested, whether they reside in a file cabinet or on a server."[227] But this does not render the warrant unconstitutional because *how* a third party searches data is irrelevant to the question of constitutionality under the Fourth Amendment.[228] Thus, the Fifth Circuit's drawing of a distinction based on the size of the database that the private third party must search is at odds with existing Fourth Amendment precedent.

B. Distinctions from General Warrants

Second, geofence warrants are distinguishable from general warrants because geofence warrants can identify the place to be searched with specificity. In contrast to the general warrants of the Colonial Era that gave the government full discretion on where to search, geofence warrants "restrict the information that is revealed to that which is closely linked to a particular crime."[229] Both modern geofence warrants and general warrants from the Colonial Era do not name a suspect,[230] but this is the pair's only similarity and is actually a feature of geofence warrants that potentially reduces police bias by limiting "the discretion of the police to select their targets in advance."[231] Additionally, this restriction on police discretion directly addresses the concerns from lower courts while still furthering the policy interests in helping police to efficiently and effectively catch suspects.[232]

Moreover, even though geofence warrants cannot identify a specific suspect, whether the suspect is known is constitutionally irrelevant.[233] The language of the Fourth Amendment states that a warrant must specify "the persons *or* things

---

225. *Seymour*, 536 P.3d at 1267, 1276 ("Although the database is large, the narrow search terms, the timeframe constraints, and the fact that the initial search was anonymized all served to minimize any invasion of privacy resulting from the search.").

226. United States v. Rhine, 652 F. Supp. 3d 38, 82 (D.D.C. 2023) (emphasis added).

227. *Id.*

228. *See id.*

229. Bambauer, *supra* note 9, at 609.

230. *Id.*

231. *Id.* at 609–10.

232. *See supra* Section II.C; *see also* United States v. Chatrie, 136 F.4th 100, 111–12 (4th Cir. 2025) (Wilkinson, J., concurring) (explaining that the "social costs" of excluding geofence location data are significant).

233. Kerr, *supra* note 14.

to be seized,"[234] and both need not be present to have a constitutional warrant.[235] For example, in *Zurcher v. Stanford Daily*, the Supreme Court found a warrant for photographs, films, and other evidence "relevant to the identity of the perpetrators of felonies" to be constitutionally sufficient.[236] The Supreme Court specifically noted that, as a constitutional matter, search warrants do not have to "name the person from whom the things will be seized" because "[s]earch warrants are not directed at persons"; rather, they "authorize the search of 'place[s]' and the seizure of 'things.'"[237] Similarly, in the internet context, "*most* warrants for Internet investigations are to identify a suspect."[238] For example, if someone sent an online threat anonymously, the government could get a warrant to trace that person's online conduct to figure out who was behind that account activity.[239] Thus, the lack of a named suspect is not constitutionally relevant and does not render geofence warrants unconstitutional.

C. Sufficiency of Warrants to Make Geofence Searches Reasonable

Third, the Supreme Court has rarely found situations in which no warrant is sufficient to make a search reasonable. One of these instances, however, occurred in *Winston v. Lee*.[240] There, the Court found that no warrant could make a "compelled surgical intrusion into an individual's body for evidence" a reasonable search.[241] If courts were to find that no warrant is sufficient to search through geofence location data, this would be a massive leap from *Winston*. It is true that geofence location data is intrusive, but it is *significantly* less intrusive than requiring a suspect to undergo surgery. As a result, applying the "no-warrant" logic of *Winston* to geofence location data would require too substantial of a leap for courts to make.

D. Public Policy Support

Further, as a public policy matter, requiring warrants would be one of the best ways to strike a balance between effective policing and protecting individuals'

---

234. U.S. CONST. amend. IV (emphasis added).

235. Zurcher v. Stanford Daily, 436 U.S. 547, 551, 554 (1978) ("In situations where the State does not seek to seize 'persons' but only those 'things' which there is probable cause to believe are located on the place to be searched, there is no apparent basis in the language of the Amendment for also imposing the requirements for a valid arrest—probable cause to believe that the third party is implicated in the crime.").

236. *Id.* at 551, 567–68.

237. *Id.* at 555 (quoting United States v. Kahn, 415 U.S. 143, 155 n. 15 (1974)).

238. Kerr, *supra* note 14; *see also* Bambauer, *supra* note 9, at 586 ("Cyberstalking, child pornography, and many other online crimes have used forms of reverse searches in order to identify the accounts associated with IP addresses that were used to engage in those crimes.").

239. Kerr, *supra* note 14.

240. 470 U.S. 753 (1985). In *Winston*, a shop owner shot "someone armed with a gun coming toward him from across the street" and wounded him on his left side. *Id.* at 755. When a suspect was found nearby with a gunshot wound to his left chest, the Commonwealth sought an order directing the suspect to "undergo surgery to remove an object thought to be a bullet lodged under his left collarbone," so that the Commonwealth could demonstrate that the bullet was fired from the shop owner's gun and thus identify the suspect as the robber. *Id.* at 756, 765.

241. *Id.* at 759, 767.

privacy in reverse warrant contexts. Any data source that is large enough—whether that be internet pen registers, keyword searches, CSLI, nearly any database query, or any other "reverse" search involving digital data[242]—would seemingly fall within the purview of these geofence decisions, so the standards for law enforcement created in the geofence context will impact "most law enforcement and national security surveillance involving the Internet."[243] As a result, the best precedent to set is one requiring law enforcement to get a warrant before collecting an individual's digital data. A warrant requirement would place a limit on law enforcement yet still allow them to use "powerful tools for investigating and deterring crime."[244] Requiring that law enforcement show probable cause and obtain a warrant also helps ensure that officers are acting in good faith and not merely haphazardly attempting to "generate leads in a completely cold case."[245] Thus, a warrant requirement would most effectively strike the balance between protecting individuals' digital data while simultaneously allowing for law enforcement to efficiently collect data when such collection is justified.

E. Prevention of Negative Alternatives

If courts decide that geofence warrants are impermissible, the government will almost certainly seek to obtain geofence location data under some other legal theory that would give law enforcement too much discretion. For example, the government might argue that geofences should be treated like checkpoint stops—with no warrant required and full discretion given to law enforcement to conduct broad-but-thin investigations that are "systematic and limited in scope."[246] Even though checkpoints require a brief "seizure" of individuals, the Supreme Court has allowed temporary checkpoints based on "some measure of individualized suspicion"[247] because the intrusion was "small enough, and the purpose well-enough tethered to the facts of a particular crime" to justify it.[248] Just as an intrusion is minimal at a checkpoint when an investigation is limited to finding information about a specific crime, the government could argue that geofences are closely tied to a crime and are merely broad-but-thin investigations, especially in the steps prior to deanonymization.

Yet while using an analysis similar to physical checkpoints might seem like a good alternative to a warrant requirement, it would not limit law enforcement discretion as much as a geofence warrant issued by a neutral magistrate who will

---

242. Kerr, *supra* note 14.

243. *Id.*

244. *See* United States v. Smith, 110 F.4th 817, 841 (5th Cir. 2024) (Ho, J., concurring) (explaining that "hamstringing the government is the whole point of our Constitution" and recognizing that geofence warrants are "powerful tools for investigating and deterring crime").

245. United States v. Brown, No. 1:16-CR-427-AT-JKL-31, 2025 WL 1674283, at *18 (N.D. Ga. June 13, 2025).

246. Jane Bambauer, *Letting Police Access Google Location Data Can Help Solve Crimes*, WASH. POST (Mar. 28, 2022), https://www.washingtonpost.com/outlook/2022/03/28/geofence-warrant-constitution-fourth-amendment/ [https://perma.cc/F78L-P5XT].

247. City of Indianapolis v. Edmond, 531 U.S. 32, 41 (2000).

248. Bambauer, *supra* note 246.

require particularized probable cause and much more than just "some measure" of suspicion.[249] In fact, courts have declined to grant applications for "unrestrained administrative inspection warrant[s]" due to a lack of particularization that makes them unconstitutional.[250] While it is relatively easy to have a systematic investigation in a physical setting such as a checkpoint, it is much harder when using digital data because the type of data and how it is stored can vary greatly. Additionally, the lack of probable cause is of particular concern because it would slide the scale too far in favor of the government at the high cost of individual citizens' privacy. Finally, individuals' ability to know whether they are being surveilled differs greatly between the checkpoint and geofence contexts. Unlike checkpoints that motorists can see as they approach, individuals cannot see the geofence that they enter, particularly because geofences by their very nature involve historical location data, similar to the historical CSLI data in *Carpenter*.[251] Therefore, this checkpoint alternative would not address the lower courts' concerns about geofence warrants providing too much discretion to law enforcement and impacting innocent individuals,[252] nor would it protect privacy rights as much as a warrant backed by particularized probable cause.

F. Summary of Points

Overall, it seems unlikely that other courts will follow the Fifth Circuit's reasoning; instead, they will likely determine that appropriately defined geofence warrants are not general warrants. While geofence warrants might not be able to provide particularized probable cause as to a specific suspect, they can still be sufficient warrants with particularity and probable cause as to the place to be searched.[253] Thus, geofence warrants and other reverse search warrants should be deemed constitutional.

VI. ALLOWING REVERSE WARRANTS WHEN COURTS HAVE DISCRETION TO DEANONYMIZE DATA AND APPROPRIATE FILTERING MECHANISMS ARE IN PLACE

The Fourth and Fifth Circuits both go too far and do not adequately balance effective policing and protection of individuals' privacy. But a middle ground exists and ought to be utilized in reverse warrant contexts, including with geofence warrants. This compromise is a filter-focused approach, which involves looking at the filter setting, the data scanned, and the output.[254] This Part argues that courts should recognize a reasonable expectation of privacy in geofence data, require the government to obtain warrants for geofence data and return to the Court prior to any deanonymization occurring, and allow geofence warrants when there is a sufficient filtering mechanism disclosed in the warrant application.

---

249. *See Edmond*, 531 U.S. at 41.

250. *In re* Sealed Search Warrant Application, 784 F. Supp. 3d 970, 976 (S.D. Tex. 2025).

251. Carpenter v. United States, 585 U.S. 296, 310 n.3 (2018).

252. *See supra* Section II.C.

253. *See* U.S. CONST. amend. IV; Kerr, *supra* note 14.

254. *See* Kerr, *supra* note 12, at 35.

A. Reasonable Expectation of Privacy in Geofence Location Data

First, courts ought to recognize a reasonable expectation of privacy in geofence location data. The third-party doctrine should not govern here, as it is ill-suited for cases in which large quantities of digital data are exposed—much like the Supreme Court found in *Carpenter*.[255] Instead, because of the large quantity of revealing data and the ability for geofences to invade and collect data from inside constitutionally protected areas,[256] courts should recognize that individuals have a reasonable expectation of privacy in their geofence location data.

Thus, law enforcement should be required to obtain a warrant that has particularized probable cause as to the place to be searched before obtaining geofence location data. At Step One, law enforcement ought to obtain a warrant in line with *Karo*: they should state exactly what data source they plan to search, the connected crime giving rise to the search of the particular area, and the length of the data collection.[257] In addition, this warrant must minimize the impact on innocent individuals by including filtering measures that narrowly tailor the geographic and temporal restrictions to the place and time of the crime, so that the results of the search are filtered to only "hit" specific individuals.[258] The exact tailoring will likely need to be established on a case-by-case basis, at least initially; but as a general rule, if the search is in an urban area, the geographic area and time period will need to be smaller compared to a search in a rural area.[259]

This method would ensure there is probable cause prior to granting a geofence warrant. The tailored "search will produce evidence useful to the government's investigation" as there would be a "fair probability" that the "suspects were inside the geofence" and using their phones, that "those phones communicated location information to Google," and that Google "can trace that information back to a particular device, accountholder, and/or subscriber."[260] As long as there is a "fair probability that contraband or evidence of a crime will be found in a particular place" and the geofence warrant is limited to the area around the crime at the time the crime occurred, courts should find probable cause.[261] Some might argue that probable cause for geofence warrants ought to be "particularized with respect to [each] person," but courts have only been this strict when physically searching or

---

255. *See supra* Subsection II.B.ii, Part IV.

256. *See supra* Part IV.

257. United States v. Karo, 468 U.S. 705, 718 (1984).

258. *See supra* Subsection II.C.ii; Kerr, *supra* note 14.

259. *See In re* Search of Info. Stored at Premises Controlled by Google, as further described in Attachment A, No. 20 M 297, 2020 WL 5491763, at *5 (N.D. Ill. July 8, 2020) (finding that the warrant location was not sufficiently tailored in part because the geofence coordinates encompassed "a congested urban area encompassing individuals' residences, businesses, and healthcare providers," and the vast majority of cell phones likely to be identified would not be relevant to any investigation (footnote omitted)); United States v. Smith, No. 3:21-CR-107-SA, 2023 WL 1930747, at *8 (N.D. Miss. Feb. 10, 2023) (finding sufficient probable cause with large geofence parameters in part because the "geofence was in a rural area where it was unlikely to return a large number of Google accounts").

260. *In re* Search of Info. that Is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 79 (D.D.C. 2021).

261. Illinois v. Gates, 462 U.S. 213, 238 (1983).

seizing a person.[262] But in the geofence context, as long as there is probable cause particularized as to the person when law enforcement is attempting to deanonymize the data, this should still meet the probable cause and particularity standards.

B. Additional Probable Cause Showing Prior to Deanonymization

Second, courts should require law enforcement to make an additional probable cause showing and obtain an additional warrant before deanonymizing the data. Once police receive the information collected at Step One of the geofence warrant, they can use that data in combination with information acquired from other investigative techniques to obtain particularized probable cause as to a specific device.[263] Requiring an additional warrant would align with other Supreme Court precedent where the Court has generally required a warrant before searching data from cell phones of specific users.[264] Additionally, this extra warrant requirement would directly address the concern expressed in lower court opinions about the amount of discretion given to law enforcement,[265] and Fourth Amendment scholars have advocated for the use of additional judicial action prior to deanonymization.[266]

C. Filtering Mechanism Requirement for Reverse Warrants

Further, courts ought to allow reverse warrants generally when there is a sufficient filter disclosed in the warrant application to limit law enforcement's discretion and reduce the impact on innocent individuals. Specifically, warrants for searches of digital data should include a filter so that the data is only provided to police when the "data matches uniquely criminal details such that there is a high probability they have engaged in criminal conduct" and the "data has been pared down to provide only relevant details about the suspected crime to the police."[267] The data ought to "refine the information that is ultimately disclosed to police by filtering out personal, irrelevant details *even about a suspect*."[268] This will reduce both the impact on innocent individuals and prevent police from diving too deeply into the intimate details of a person without a warrant—two of the main concerns expressed by lower courts when analyzing the geofence warrants.[269] In the geofence warrant context, this filtering would include limiting the time period and geographic area requested so as to only identify those most likely involved in the crime. As another example, in the reverse keyword search context, the police should include a limited number of specific keywords, and the private party responding to the warrant

---

262. Ybarra v. Illinois, 444 U.S. 85, 91 (1979).

263. United States v. Smith, 110 F.4th 817, 825 (5th Cir. 2024) (explaining that investigative techniques can include cell phone tracking or "sending out additional warrants tailored to the specific information received"); United States v. Brown, No. 1:16-CR-427-AT-JKL-31, 2025 WL 1674283, at *18 (N.D. Ga. June 13, 2025).

264. Riley v. California, 573 U.S. 373, 386 (2014) (holding that "officers must generally secure a warrant before conducting such a search" of data on a cell phone during a search incident to a lawful arrest).

265. *See supra* Section II.C.

266. For example, Professor Jane Bambauer has argued that law enforcement should obtain a warrant "before any identifying data is revealed." Bambauer, *supra* note 9, at 609.

267. *Id.* at 580.

268. *Id.* at 581.

269. *See supra* Section II.C.

ought to filter the data so that only the most relevant details are provided to law enforcement.[270] But this data should remain anonymous unless and until law enforcement can develop probable cause using the results combined with other investigative techniques.[271] After a neutral magistrate determines there is sufficient probable cause for a warrant, law enforcement should be able to obtain the deanonymized data resulting from the reverse keyword search. This idea—searching for and using filters to obtain specific data and only providing identifying information to law enforcement upon an additional showing of probable cause—can be implemented for all reverse search warrants. Such a model not only best protects individuals from unnecessary intrusion into intimate parts of their lives but also substantially eliminates concerns about law enforcement having too much discretion.

CONCLUSION

While modern Fourth Amendment caselaw involving technology has been developing over the last 50 years, there is only limited caselaw on how the third-party doctrine applies to digital data and technology. With the increasing use of geofence warrants in recent years, courts have begun grappling with how to analyze issues involving third-party location data. But geofence warrants are just the tip of the iceberg, and the impacts of these decisions will be immense. The solution that best balances individual privacy interests and public interests in effective policing is recognizing a reasonable expectation of privacy in geofence location data and imposing a warrant requirement. Specifically, these reverse warrant applications ought to detail a filtering mechanism to limit the results provided by the private party. Additionally, courts should require that the government seek an additional warrant supported by probable cause before the private party can provide any identifying information. Since this approach best balances the interests of law enforcement and individuals' privacy, the filter-focused analysis should govern in all reverse search warrant contexts.

---

270. *See In re* Geo-Fence & Cell Site Location Info. Search Warrants, No. CM22000505-01, 2022 WL 22916777, at *1, *3 (Va. Cir. Ct. July 28, 2022) (finding that a warrant based on a particular search term was constitutionally permissible because the "search term was a specific, unique, not-easily confused search term entered during an unusual time of the day and for a limited period that would, more probably than not, be related to the specific crime under investigation").

271. *See* United States v. Brown, No. 1:16-CR-427-AT-JKL-31, 2025 WL 1674283, at *18 (N.D. Ga. June 13, 2025).