Congressional Research Service
Informing the legislative debate since 1914

Geofence and Keyword Searches: Reverse Warrants and the Fourth Amendment

February 10, 2026

Congressional Research Service
https://crsreports.congress.gov
R48852

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Geofence and Keyword Searches: Reverse Warrants and the Fourth Amendment

SUMMARY

R48852

February 10, 2026

Peter G. Berris
Legislative Attorney

Clay Wild
Legislative Attorney

From thermal imaging and wiretaps to Global Positioning System (GPS) tracking and various forms of electronic eavesdropping, law enforcement's use of emerging technologies is sometimes in tension with constitutional privacy protections. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 29 (2001) ("This case presents the question whether the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment."); Olmstead v. United States, 277 U.S. 438, 455 (1928) (examining whether "evidence of private telephone conversations between the defendants and others, intercepted by means of wire tapping, amounted to a violation of the Fourth and Fifth Amendments"). Over the past century, federal courts have considered the extent to which the Fourth Amendment's prohibition of unreasonable searches and seizures limits law enforcement's use of such technologies. *See, e.g.*, *Kyllo*, 533 U.S. at 2; *Olmstead*, 277 U.S. at 455. In 2026, the Supreme Court granted certiorari to consider the constitutionality of searches and warrants involving a relatively new, technology-assisted law enforcement tool—geofences. Chatrie v. United States, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026). Some state courts have opined on the constitutionality of similar investigatory tools, including those known as keyword warrants. *E.g.*, People v. Seymour, 536 P.3d 1260 (Colo. 2023).

Both geofence and keyword warrants are sometimes described as *reverse warrants*. Using a reverse warrant, law enforcement essentially works backwards from the traditional process of identifying a known suspect and then obtaining a search warrant to gather information on that suspect. Instead, with a reverse warrant, law enforcement first identifies facts that may constitute incriminating evidence, such as the time and location of a crime or an internet search for an address where a crime occurred. Law enforcement then attempts to identify a suspect by compelling user information correlating to those facts from a technology provider. *See, e.g.*, *id.* at 1268 (describing how and why law enforcement obtained keyword warrant); *see also* United States v. Smith, 110 F.4th 817, 826 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025) (describing law enforcement use of geofence warrant in particular case).

The use of reverse warrants, particularly geofence warrants, has garnered media attention and legislative interest at the state and federal levels. In 2023, Google announced that it would reduce the default length of time it stores the location information typically sought by geofence warrants. It also announced that it would migrate user data from internal servers to users' individual devices, which could effectively make it impossible for Google to share user location data with law enforcement. The move drew interest from some observers who believe it could significantly curtail the use of geofence warrants, although at least one federal appellate court has observed that, as of 2024, the government was still seeking geofence data from Google. *Smith*, 110 F.4th at 822 n.3. Law enforcement may also continue to seek geofence data or other information covered in this report from other companies.

This report examines evolving legal issues regarding reverse warrants. It summarizes Fourth Amendment principles and the caselaw surrounding reverse warrants. The report concludes with considerations for Congress.

Contents

Tables

Contacts

Introduction

When law enforcement obtains a search warrant, they are traditionally focused on a "known suspect."[1] After a robbery, for example, law enforcement may be able to identify a suspect based on information gathered from witnesses or from physical evidence like fingerprints found in a recovered getaway vehicle.[2] From there, they may seek to obtain a warrant to search the dwelling of the robbery suspect if there is probable cause that evidence of that crime (e.g., stolen currency) will be found there.[3]

Sometimes, however, law enforcement may know the approximate time and location of a robbery but not the identities of any suspects.[4] These conditions may prompt law enforcement to try to identify suspects through the execution of what has become known as a *reverse warrant*. With a reverse warrant, law enforcement essentially works backwards from a "potentially incriminating piece of evidence" and looks for user information "implicated by that evidence" to identify a suspect.[5] In other words, according to one court, in a typical search warrant, police might "seek information *on* a particular suspect," but with a reverse warrant, police might instead "seek information that would *lead* to the identity of a suspect."[6] Reverse warrants are relatively new, and two prominent emerging forms of such warrants are geofence warrants and keyword warrants.[7] In executing a geofence warrant, law enforcement compels a company to provide certain information identifying the particular smartphones that were present within a geographic area during a specified time frame.[8] Law enforcement can then use the information to potentially identify the owners of any smartphones found in the area of interest during the time frame.[9] With

[1] United States v. Smith, 110 F.4th 817, 822 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025) (quoting United States v. Rhine, 652 F. Supp. 3d 38, 66 (D.D.C. 2023)) (explaining how reverse warrants differ from "traditional search warrants").

[2] *E.g.*, United States v. Jackson, 756 F.2d 703, 705 (9th Cir. 1985).

[3] *Id.* ("It was a reasonable inference that [the Defendant] might keep stolen currency in his apartment from a bank robbery two months earlier . . . . The magistrate's substantial basis for concluding that probable cause existed is apparent."). More information about warrants, the Fourth Amendment, and the Federal Rules of Criminal Procedure may be found in CRS Legal Sidebar LSB11165, *Disrupting Botnets: An Overview of Seizure Warrants and Other Legal Tools*, by Peter G. Berris (2024).

[4] *Smith*, 110 F.4th at 822; *see also* United States v. Chatrie, 590 F. Supp. 3d 901, 905 (E.D. Va. 2022), *aff'd*, 107 F.4th 319, 325 (4th Cir. 2024), *aff'd en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam) (describing when officers turned to geofence warrant in underlying case), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (mem.).

[5] People v. Seymour, 536 P.3d 1260, 1268 n.1 (Colo. 2023).

[6] *In re* Search of Info. that is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 84 n.19 (D.D.C. 2021) (mem.) (emphasis added).

[7] *See, e.g.*, *Reverse Search Warrants*, NAT'L ASS'N OF CRIM. DEF. LAWYERS, https://www.nacdl.org/Landing/Reverse-Search-Warrants [https://perma.cc/7VN6-HE7N] (last visited Aug. 25, 2025) (describing "reverse search warrants" as including "geofence warrants and keyword search warrants"); *cf. In re Search of Info. that is Stored at the Premises Controlled by Google LLC*, 579 F. Supp. 3d at 84 n.19 ("Some of the public criticism directed toward geofence warrants is that they fall into the category of so-called 'reverse warrants,' which do not seek information on a particular suspect, but rather seek information that would lead to the identity of a suspect, compromising third parties' privacy interests in the process.").

[8] *Smith*, 110 F.4th at 822.

[9] This typically involves a three-step process that begins with anonymized information, and ultimately may yield deanonymized data as well. *See infra* **Table 1**.

a keyword[10] warrant, law enforcement obtains the account information of users who entered a particular search term into a search engine, such as the address where a crime occurred.[11]

Caselaw on reverse searches is scarce.[12] Much of this limited body of jurisprudence focuses on geofence warrants,[13] likely because such warrants have, in some recent years, numbered in the thousands.[14]

Legal challenges to the constitutionality of such warrants remain pending,[15] and the caselaw that does exist tends to focus on two fundamental questions. The first is whether the collection and subsequent review of data pursuant to a reverse warrant is in itself a "search" implicating the protections of the Fourth Amendment. If it is a search, the second question is whether a properly issued warrant is sufficient protection under the Fourth Amendment to permit the use of the seized data as evidence.

Given congressional interest in the intersection of law enforcement and technology,[16] this report examines select legal issues that may arise in investigations and prosecutions involving reverse warrants, with a focus on geofence and keyword warrants. The report first provides background on jurisprudence involving the Fourth Amendment and technology. It then analyzes the procedures typically employed by a company in response to both, the scant caselaw that exists regarding these types of warrants, and the constitutional issues present. The report concludes with some considerations for Congress.

[10] Given the relatively new emergence of these warrants, the terminology used to discuss them is sometimes inconsistent. For simplicity's sake, this report uses "keyword warrants" to describe those executed in accordance with the procedures described *infra*, "Keyword Warrants." "Keyword warrants," as used in this report, does not refer to warrants for a known individual's search history.

[11] People v. Seymour, 536 P.3d 1260, 1268 n.1 (Colo. 2023). As with geofence warrants, this typically involves a multistep process, discussed below. *See infra* "Policies and Procedures."

[12] *See Smith*, 110 F.4th at 821 ("As a relic of their novelty, '[t]here is a relative dearth of case law addressing geofence warrants.'" (quoting United States v. Chatrie, 590 F. Supp. 3d 901, 906 (E.D. Va. 2022))); *Seymour*, 536 P.3d at 1269 ("The constitutionality of reverse-keyword warrants presents an issue of first impression in Colorado. Indeed, to our knowledge, no state supreme court or federal appellate court has addressed the constitutionality of such warrants.").

[13] *But see, e.g.*, *Seymour*, 536 P.3d at 1267–68 (examining keyword warrants).

[14] *See infra* **Table 1**. As discussed below, a policy change at the company that receives the most geofence warrants (Google) may affect their prevalence moving forward. *See* discussion *infra* notes 88–93.

[15] *See, e.g.*, Chatrie, 590 F. Supp. 3d at 905, *aff'd*, 107 F.4th 319, 325 (4th Cir. 2024), *aff'd en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

[16] *E.g.*, Letter from Rep. Jim Jordan, Chairman, H. Judiciary Comm., to Merrick Garland, Att'y Gen., U.S. Dep't of Just. (Aug. 10, 2023), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/2023-08-10-jdj-to-doj-re-geofencing.pdf [https://perma.cc/D2N4-HWZN] (describing oversight efforts on "how federal law enforcement uses geofence warrants"); Press Release, Alex Padilla, Senator, U.S. Senate, Padilla Calls on Google to Limit Collection and Storage of Location Data as Republicans Seek to Criminalize Abortion (May 25, 2022), https://www.padilla.senate.gov/newsroom/press-releases/padilla-calls-on-google-to-limit-collection-and-storage-of-location-data-as-republicans-seek-to-criminalize-abortion%EF%BF%BC/#:~:text=WASHINGTON%2C%20D.C.,obtain%20reproductive%20health%20care [https://perma.cc/N6EL-U25H].

Background: Technology and the Fourth Amendment

The Fourth Amendment limits searches and seizures by the government.[17] Some law enforcement efforts to obtain information constitute a search or a seizure within the meaning of the Fourth Amendment as it is interpreted by courts, but others may not.[18] In determining whether a particular means of gathering information—such as the use of a geofence—constitutes a "search" triggering Fourth Amendment protections, federal courts generally look to whether the government action involves physical intrusion into a constitutionally protected area[19] or violates a person's "subjective expectation of privacy that society recognizes as reasonable."[20]

A variety of considerations informs whether an expectation of privacy is reasonable, but the Supreme Court has held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[21] This concept—known as the "third-party doctrine"[22]—reflects a judgment that a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[23] In articulating this doctrine, the Supreme Court in 1976 concluded that a bank customer lacked a reasonable expectation of privacy in financial records stored with his bank by virtue of his being a customer there.[24] Three years later, the Court concluded that there was no reasonable expectation of privacy in numbers dialed on a landline telephone because "telephone users realize that they must 'convey' phone numbers to the telephone company" and in so doing they "assume[] the risk" that the information may be revealed to the police.[25]

Given the ubiquity of computers and smartphones, and the omnipresence of the internet in the modern era,[26] a strict application of the third-party doctrine may have different implications today

[17] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."). For a discussion of the "state action doctrine," which applies Fourth Amendment protections to the actions of private parties when they act as an instrument or agent of the government, see CRS Legal Sidebar LSB10713, *The Fourth Amendment and the Internet: Legal Limits on Digital Searches for Child Sexual Abuse Material (CSAM)*, by Michael A. Foster (2022). Other discussions of Fourth Amendment jurisprudence in various contexts may be found in additional CRS products. *See infra* **Table 3**.

[18] *Compare* Katz v. United States, 389 U.S. 347, 348, 353 (1967) (holding FBI agents' use of an electronic listening and recording device to surveil a public telephone booth constituted a search), *with* Oliver v. United States, 466 U.S. 170, 179 (1984) (reasoning open fields "do not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from government interference or surveillance").

[19] United States v. Jones, 565 U.S. 400, 407 n.3 (2012) ("Where . . . the Government obtains information by physically intruding on a constitutionally protected area . . . a search has undoubtedly occurred.").

[20] Kyllo v. United States, 533 U.S. 27, 33 (2001); *see also* Smith v. Maryland, 442 U.S. 735, 740 (1979) (similar); Cong. Rsch. Serv., *Katz and Reasonable Expectation of Privacy Test*, CONSTITUTION ANNOTATED, https://constitution.congress.gov/browse/essay/amdt4-3-3/ALDE_00013717/ (last visited Feb. 24, 2025) (providing overview of caselaw concerning expectations of privacy).

[21] *Smith*, 442 U.S. at 743–44; *accord* Carpenter v. United States, 585 U.S. 296, 304 (2018).

[22] United States v. Trader, 981 F.3d 961, 967 (11th Cir. 2020).

[23] United States v. Miller, 425 U.S. 435, 443 (1976).

[24] *Id.*

[25] *Smith*, 442 U.S. at 742, 744.

[26] *See* Press Release, U.S. Census Bureau, Computer and Internet Use in the United States: 2021 (June 18, 2024), https://www.census.gov/newsroom/press-releases/2024/computer-internet-use-2021.html [https://perma.cc/E69B-
(continued...)

than it did in the 1970s. Under a broad construction of the doctrine, a potentially vast amount of digital information would fall outside the protections of the Fourth Amendment, because such information is often shared by customers with technology providers in the ordinary course of using a product.[27]

The use of new technological investigative techniques by law enforcement has resulted in a series of Supreme Court opinions reexamining the contours of the Fourth Amendment with respect to emerging technologies and, in one case, limiting the scope of the third-party doctrine. In the 2012 opinion *United States v. Jones*, the Supreme Court evaluated the application of the Fourth Amendment to Global Position System (GPS) tracking devices.[28] There, law enforcement affixed a GPS device to a suspect's car without a warrant and monitored the vehicle's movements for 28 days.[29] The Court held that by attaching the GPS device to the vehicle, law enforcement "physically occupied private property for the purpose of obtaining information,"[30] which amounted to a Fourth Amendment search. Across two separate concurrences, five Justices agreed that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[31]

Two years after *Jones*, the Supreme Court issued its opinion in *Riley v. California*, recognizing the unique privacy implications resulting from digital searches of cell phones.[32] The *Riley* Court distinguished cell phones from other objects that a person might carry in light of the pervasiveness of the technology, the "immense storage capacity" of "modern cell phones," the large variety of types of information that phones contain, and the prolonged period of time that information may cover.[33] With a cell phone, the Court wrote, the "sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."[34]

In 2018, the Supreme Court decided *Carpenter v. United States*,[35] which involved the warrantless search of historical cell-site location information (CSLI)—data that record the location of a cellular device when it connects to "a set of radio antennas called 'cell sites'" typically mounted on towers or structures.[36] In *Carpenter*, law enforcement obtained a defendant's CSLI covering 127 days from cellular providers through a court order issued pursuant to the Stored Communications Act (SCA; discussed in **Table 2** below).[37] The *Carpenter* Court held that the CSLI was not exempt from Fourth Amendment protection pursuant to the third-party doctrine,

J3DC] ("Most U.S. households had at least one type of computer (95%) and had a broadband internet subscription (90%) in 2021, an increase from 2018 (92% and 85%, respectively)."). According to the Census Bureau, "Smartphones were the most common computing device in U.S. households (90%), followed by desktop or laptop computers (81%) and tablets (64%) in 2021." *Id*.

[27] *See* S. REP. NO. 99-541, at 3 (1986) (discussing the proliferation of computers and the result that categories of electronic "information may be subject to no constitutional privacy protection" because they are "subject to control by a third party computer operator").

[28] 565 U.S. 400 (2012).

[29] *Id.* at 403.

[30] *Id.* at 404.

[31] *Id.* at 415 (Sotomayor, J., concurring); *id*. at 420 (Alito, J., concurring).

[32] 573 U.S. 373 (2014).

[33] *Id*. at 393–95.

[34] *Id.* at 394.

[35] 585 U.S. 296 (2018).

[36] *Id.* at 300.

[37] *Id.* at 301–02; *infra* **Table 2**.

even though the CSLI was shared by the defendant with cellular providers in the course of his cell phone use.[38] The Court rejected the idea that the defendant's sharing of CSLI with the providers was voluntary. Echoing the Court's concerns in *Riley*, the *Carpenter* Court observed that "[c]ell phone location information is not truly 'shared' as one normally understands the term" given that carrying a cell phone is "indispensable to participation in modern society" and "a cell phone logs a cell-site record by dint of its operation."[39] In addition, the Court concluded that the defendant had a reasonable expectation of privacy in the CSLI in light of the revealing nature of the information at issue, which the Court observed amounted to "near perfect surveillance" because cell phones accompany their owners in nearly every physical space and because the CSLI is both precise and retrospective.[40] As the Court in *Carpenter* put it, CSLI can provide "an intimate window into a person's life, revealing not only his particular movements, but through them, his 'familial, political, professional, religious, and sexual associations.'"[41] Nevertheless, the Court described its holding as a "narrow" one that did not abolish the third-party doctrine or predetermine its application to other technological surveillance.[42] At least some federal courts have been reluctant to extend *Carpenter* to other digital contexts.[43]

Table 1. Cell Tower Dumps

Some federal courts have examined whether the *Carpenter* exception to the third-party doctrine extends to cell tower dumps, or "a download of information on all the devices that connected to a particular cell-site during a particular interval."[44] As one court explained, "In a tower dump . . . law enforcement identifies the cell towers near the scene of a crime and seeks 'a list of the telephone numbers that connected to the cell towers during the pertinent time period,' along with date, times, and telephone numbers for connecting calls."[45] In other words, while historical CSLI is "narrowly targeted" towards a particular person but "quite expansive as to that person," tower dumps "are narrow as to the individual suspect—they typically seek location data, cell numbers, and subscriber information—but are broad as to third-party data, collecting all phone numbers for users who connected to the relevant cell towers."[46]

The *Carpenter* Court expressly declined to weigh in on the constitutionality of tower dumps,[47] and federal courts have split on the issue.[48] A federal district court in Michigan concluded that there is no reasonable expectation of privacy in five hours' worth of short-term CSLI disclosed via a tower dump, since it "was magnitudes short of the seven days of close location tracking in *Carpenter*."[49] In other words, that court rejected the idea that the tower dump provided the comprehensive chronicle of past movements that troubled the *Carpenter* Court.[50] At least one federal court reached a different conclusion, holding that there is a reasonable expectation of privacy in short-term CSLI revealed through a tower dump, triggering the warrant requirement under the Fourth Amendment (although that court ultimately affirmed the collection of tower dump data in question under the good faith

[38] *Id.* at 309–10.

[39] *Id.* at 315.

[40] *Id.* at 311–12.

[41] *Id.* at 311 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[42] *Id.* at 316.

[43] *See infra* "Is the Collection of Geofence Data a "Search"?"

[44] *Carpenter*, 585 U.S. at 316.

[45] United States v. Medina, 712 F. Supp. 3d 226, 237 (D.R.I. 2024), *vacated and remanded on other grounds*, 125 F.4th 310 (1st Cir. 2025) (quoting *In re* Application of the U.S.A. for an Ord. Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT&T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless, 42 F. Supp. 3d 511 (S.D.N.Y. 2014)).

[46] *Id.* at 238.

[47] *Carpenter*, 585 U.S. at 316.

[48] *See, e.g.*, United States v. Pricop, 775 F. Supp. 3d 1036, 1038–39 (D. Ariz. 2025) (collecting cases).

[49] United States v. Williams, 741 F. Supp. 3d 642, 650 (E.D. Mich. 2024).

[50] *Id.*

exception, discussed below).[51] The court concluded that tower dumps provide "'near perfect surveillance' of a population at a moment in time," reveal intimate information, and provide a cheap and efficient investigative technique that "would be impossible to do with traditional surveillance."[52]

Geofence Warrants

Geofences have been described as electronic systems that establish a virtual perimeter around a specific geographic location.[53] Private companies use geofences for business purposes such as targeted advertising.[54] Geofence warrants are an investigative tool employed by law enforcement to gather location information revealing which smartphones were at or near the scene of a crime when it was committed.[55] Law enforcement has used geofence warrants to investigate criminal matters ranging from homicides[56] to "stolen pickup trucks and smashed car windows."[57] The scope of geofence warrants has varied as well. Some geofence warrants have covered geographical areas measured in feet or meters;[58] others have encompassed areas larger than an acre.[59] Temporally, some have been limited to minutes or hours;[60] others have covered a period of days.[61] For example, in one case law enforcement used a geofence warrant to obtain information from Google that ultimately revealed the identities of individuals who were present at the scene of a robbery of a postal service employee.[62] The warrant sought Location History[63] data corresponding to a one-hour period during which the robbery occurred and "a geofence covering approximately 98,192 square meters" surrounding the scene of the crime.[64] The acquired information enabled law enforcement not only to identify the individuals present at the scene, but

[51] *Medina*, 712 F. Supp. 3d at 246, 248; *infra* notes 95–97 and accompanying text.

[52] *Id.* at 242–43 (quoting *Carpenter*, 585 U.S. at 309–13). A number of state courts have considered cell tower dumps. *See, e.g.*, Commonwealth v. Kurtz, 294 A.3d 509, 530 (Pa. Super. Ct. 2023) (holding that defendant had no legitimate expectation of privacy concerning tower dump data produced to law enforcement by AT&T), *aff'd on other grounds*, Nos. 98 MAP 2023, 99 MAP 2023, 100 MAP 2023, 2025 WL 3670767 (Pa. Dec. 16, 2025); State v. Bryant, No. A-1399-24, 2025 WL 3481348, at *7 (N.J. Super. Ct. App. Div. Dec. 4, 2025) (holding that "tower dump searches can be constitutional, but they need a warrant, and the warrant must be particularized and supported by probable cause"); Commonwealth v. Perry, 184 N.E.3d 745, 752 (Mass. 2022) (examining legality of tower dumps under Massachusetts law).

[53] Brian L. Owsley, *The Best Offense is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 HOFSTRA L. REV. 829, 832 (2022).

[54] *Id.*

[55] *Chatrie*, 590 F. Supp. 3d at 905, *aff'd*, 107 F.4th 319, 325 (4th Cir. 2024), *aff'd en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026). In this sense, geofence warrants share some conceptual similarities with cell tower dumps, discussed above. *See supra* **Table 1**.

[56] State v. Contreras-Sanchez, 5 N.W.3d 151, 156 (Minn. Ct. App. 2024).

[57] United States v. Smith, 110 F.4th 817, 822 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025).

[58] *Contreras-Sanchez*, 5 N.W.3d at 156; *Chatrie*, 107 F.4th at 324.

[59] *In re* Search of Info. that is Stored at Premises Controlled by Google, No. 2:22-MJ-01325, 2023 WL 2236493, at *10 (S.D. Tex. Feb. 14, 2023).

[60] *Chatrie*, 107 F.4th at 324; *In re* Search of Info. that is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d. 62, 72 (D.D.C. 2021).

[61] *Contreras-Sanchez*, 5 N.W.3d at 158.

[62] *Smith*, 110 F.4th at 826.

[63] For clarity, this report capitalizes the term "Location History" when referring to Google Location History information, described below. *See infra* notes 70–79, 88–93 and accompanying text.

[64] *Id.* at 827.

also to ascertain the precise time that the individuals were there and, accordingly, establish evidence of their involvement in the crime.[65]

Google has reportedly been the primary recipient of geofence warrants.[66] In 2019, Google received roughly 9,000 geofence requests from law enforcement, and by 2021, more than 25% of all warrants that Google received in the United States were for geofence data.[67] For comparison, Apple reported receiving 36 geofence warrants from law enforcement in 2022[68] and 26 in 2023.[69] Google's centrality in the phenomenon of geofence warrants is "in large part due to its extensive Location History database known as the 'Sensorvault.'"[70] According to Google, Location History is "a history or journal that [its] users can choose to create, edit, and store to record their movements and travels."[71] Google users are not automatically subject to the collection of their Location History: Google users must agree to have their Location History monitored.[72] As of October 2018, Google estimated that approximately one-third of its users, equating to 592 million individuals, had opted in to share their Location History.[73] Location History allows Google to "'potentially locate an individual within about sixty feet or less,' and in certain circumstances, down to three meters."[74] Location History may even be able to ascertain a particular device's elevation, including what floor of a building it is on.[75] Location History does not, however, determine an individual's location with "absolute precision."[76] Rather, specific datapoints in a device's Location History are reported with a "confidence interval,"[77] which reflects Google's confidence in the accuracy of the estimated locations. As summarized by the United States Court of Appeals for the Fifth Circuit,[78] "[t]he smaller the radius, the more confident Google is in th[e] phone's exact location."[79]

---

[65] *Id.* at 820.

[66] *Id.* at 822.

[67] *Id.* at 821–22.

[68] APPLE INC., APPLE TRANSPARENCY REPORT: GOVERNMENT AND PRIVATE PARTY REQUESTS, JANUARY 1-JUNE 30, 2022 tbl. 11 (2022), https://www.apple.com/legal/transparency/pdf/requests-2022-H1-en.pdf#page=14 [https://perma.cc/7PRN-JPLP]; APPLE INC., APPLE TRANSPARENCY REPORT: GOVERNMENT AND PRIVATE PARTY REQUESTS, JULY 1-DECEMBER 31, 2022 tbl. 14 (2022), https://www.apple.com/legal/transparency/pdf/requests-2022-H2-en.pdf#page=16 [https://perma.cc/T378-Z3BX].

[69] APPLE INC., APPLE TRANSPARENCY REPORT: GOVERNMENT AND PRIVATE PARTY REQUESTS, JANUARY 1-JUNE 30, 2023 tbl. 14 (2023), https://www.apple.com/legal/transparency/pdf/requests-2023-H1-en.pdf#page=17 [https://perma.cc/5ZVB-VQVC]; APPLE INC., APPLE TRANSPARENCY REPORT: GOVERNMENT AND PRIVATE PARTY REQUESTS, JULY 1-DECEMBER 31, 2023 tbl. 14 (2023), https://www.apple.com/legal/transparency/pdf/requests-2023-H2-en.pdf#page=17 [https://perma.cc/WCQ8-4AZS].

[70] *Smith*, 110 F.4th at 822.

[71] Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from "Geofence" General Warrant at 6, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19-CR-00130), Dkt. No. 59-1.

[72] *Id.* at 835.

[73] *Id.* at 823.

[74] *Id.* at 823 (quoting Owsley, *supra* note 53, at 835).

[75] *Id.* at 824.

[76] *Id.*

[77] *Id.*

[78] This report references decisions by federal appellate courts of various regional circuits. For purposes of brevity, references to a particular circuit in this report (e.g., the Fifth Circuit) refer to the U.S. Court of Appeals for that particular circuit (e.g., the U.S. Court of Appeals for the Fifth Circuit).

[79] *Smith*, 110 F.4th at 824.

Google's Policies and Procedures Regarding Geofence Warrants

In practice, the unsettled legal terrain surrounding geofence warrants (discussed more below) has meant that the procedures for executing them have been driven in large part by the corporate policies of Google.[80] Under Google's three-step process for geofence requests, law enforcement must first obtain a judicial warrant "compelling Google to disclose an anonymized list of all Google user accounts" with saved Location History information corresponding to a specified geographic area and time frame.[81] Second, after the government reviews the information provided by Google at step one, it "can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request."[82] Given the loosened "geographical and temporal limits" on the scope of information at step two, "Google generally requires law enforcement to narrow its request for this more expansive location data to only a subset of the users pinpointed in Step One."[83] Third, "the government can compel Google to provide account-identifying information," such as account holder names and email addresses, associated with the anonymized device numbers that law enforcement has identified as relevant under step two.[84] What it actually means to "compel" Google beyond step one seems to vary in practice. In one case, the United States Postal Inspection Service relied on the initial search warrant to compel Google at all three steps.[85] By contrast, a county detective in Minnesota obtained an additional warrant to compel deanonymized data from Google at step three.[86] Google has described the three-step process as "typically" followed, while some contend that it is often subject to case-specific negotiations between law enforcement and Google.[87]

Google's policies with respect to data collection and storage also have an impact on the amount of data that is available for law enforcement to obtain in the first place. In 2023, Google announced that it reduced the default length of its storage of Location History from 18 months to three months.[88] Google also said that it would store Location History on user devices rather than in the Sensorvault.[89] Some observers believe these changes could significantly curtail the use of

[80] *Id.*

[81] Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from "Geofence" General Warrant at 12, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19-CR-00130), Dkt. No. 59-1.

[82] *Id.* at 13.

[83] United States v. Chatrie, 107 F.4th 319, 324 (4th Cir. 2024), *aff'd en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

[84] Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from "Geofence" General Warrant at 14, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19-CR-00130), Dkt. No. 59-1.

[85] United States v. Smith, 110 F.4th 817, 828 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025).

[86] State v. Contreras-Sanchez, 5 N.W.3d 151, 159 (Minn. Ct. App. 2024).

[87] *See* Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from "Geofence" General Warrant at 14, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19-CR-00130), Dkt. No. 59-1; *see also* Brief for Technology Law and Policy Clinic at New York University School of Law & Electronic Frontier Foundation as Amici Curiae in Support of Defendant-Appellant at 15–16, United States v. Chatrie, 107 F.4th 319 (4th Cir. 2024) (No. 22-4489), 2023 WL 1368629 (contending that "[t]he variability of Google's compliance practices further attests to the three-step procedure's unreliability as a guardrail against police discretion. Even Google presents the three-step procedure as a policy that is 'typically' followed, not stringently observed.").

[88] 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/9Y4K-ACJL].

[89] *Id.*; Google said that it would allow users to back up that data in the cloud, where it would be "automatically

(continued...)

geofence warrants.[90] Still, litigation on geofence warrants that predate the policy change remains pending, and at least one federal appellate court has observed that geofence warrants remain logistically viable even if their scope and frequency might be diminished.[91] For example, law enforcement might seek a geofence warrant from a company other than Google.[92] In addition, caselaw on geofence warrants may inform subsequent litigation over other forms of reverse searches such as keyword warrants, as discussed below.[93]

Constitutionality of Geofence Searches

As previously discussed, determining the constitutionality of geofence searches typically involves two discrete analyses—whether the collection of geofence data itself constitutes a Fourth Amendment search, and if so, whether a judicial warrant provides satisfactory protection under the Fourth Amendment. This section discusses the courts' consideration of these questions.

Is the Collection of Geofence Data a "Search"?

In 2024, the Fourth and Fifth Circuits issued diverging opinions on whether the collection of geofence data amounts to a Fourth Amendment search. In *United States v. Chatrie*, the district court denied the defendant's motion to suppress geofence evidence.[94] Although the district court concluded that the underlying geofence warrant "plainly" violated the Fourth Amendment, it declined to exclude the evidence pursuant to the "good faith" exception to the Fourth Amendment.[95] That exception does not require the exclusion of evidence garnered by "officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be unsupported by probable cause."[96] The underlying rationale is that excluding evidence in such a scenario would not have a "deterrent effect when the offending officers acted in the objectively reasonable belief that their conduct did not violate the Fourth Amendment."[97]

On appeal, a Fourth Circuit panel, declining to extend *Carpenter* to a search of Google's Location History information, concluded that the defendant lacked a reasonable expectation of privacy in

encrypt[ed] . . . so no one can read it, including Google." *See also* Lars Daniel, *Google to Stop Giving Location Evidence to Law Enforcement*, FORBES, June 14, 2025 (describing Google policy shift).

[90] *See Smith*, 110 F.4th at 822 n.3.

[91] *Id.*; *compare* Petition for Writ of Certiorari at 10, Chatrie v. United States, No. 25-112 (U.S. July 28, 2025) ("Though Google announced that it intended to make this change gradually over the year between 2023 and 2024, petitioner is not aware of any subsequent announcements that the change has been made, detailing how the change affects legacy Google devices, or specifying which data Google continues to collect. Geofence warrants continue to be litigated."), *with* Brief for the United States in Opposition at 18, Chatrie v. United States, No. 25-211 (U.S. Nov. 24, 2025). ("This Office has been informed that all Location History data was deleted from Google's Sensorvault database by the end of July 2025. Accordingly, it is the government's understanding that Google will be unable to respond to geofence warrants going forward, except to the extent that Google retains data responsive to specific geofence warrants or geofence preservation requests received before that date.").

[92] *See* discussion *infra* notes 68–69; *see also Smith*, 110 F.4th at 822 n.2 (stating that "Companies such as Apple, Lyft, Snapchat, and Uber have all received geofence warrant requests.") (citing Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2512–13 (2021)).

[93] *See infra* "Keyword Warrants."

[94] United States v. Chatrie, 590 F. Supp. 3d 901, 905, 918–19 (E.D. Va. 2022), *aff'd*, 107 F.4th 319, 325 (4th Cir. 2024), *aff'd en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

[95] *Id.* at 905, 925 (quoting United States v. Leon, 468 U.S. 897 (1984)).

[96] *Leon*, 468 U.S. at 900.

[97] *Id.* at 918.

that information.[98] First, the court determined that because the geofence warrant at issue sought only two hours of Location History, the privacy implications were far more limited than they were with the CSLI at issue in *Carpenter* or the GPS monitoring in *Jones*.[99] Second, the Fourth Circuit panel said that Location History, unlike CSLI, is voluntarily shared because it "is off by default and can be enabled only by a user's affirmative act."[100] Thus, the Fourth Circuit panel held that the third-party doctrine applied.[101]

However, in November of 2024, the Fourth Circuit ordered rehearing of *Chatrie en banc* and subsequently heard arguments on January 30, 2025.[102] The court vacated the first *Chatrie* panel's judgment and opinion on appeal,[103] and on April 30, 2025, the *en banc* court issued a one-line *per curiam* opinion, affirming the judgment of the district court.[104]

The *en banc* Fourth Circuit "fractured"[105] in its reasoning, in what the Chief Judge described as a "labyrinth" of eight separate concurrences and one dissent, representing "widely divergent views on the intersection of the Fourth Amendment and the groundbreaking investigative tool at issue here."[106] Fourteen of the Circuit's fifteen judges joined the *per curium* opinion.[107] A majority of the *en banc* court (across several opinions) agreed that the officers benefited from the good faith exception.[108] Nearly half of the *en banc* court would have concluded that the collection of geofence data was not a Fourth Amendment search under various theories, including application of the third-party doctrine.[109] By contrast, several other members of the *en banc* court analogized geofence information to the CSLI protected by *Carpenter* and would have held that it is subject to

[98] *Chatrie*, 107 F.4th at 324.

[99] *Id.* at 330.

[100] *Id.* at 332.

[101] *Id.*

[102] United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026). For additional discussion of the significance of *en banc* rehearings, see CRS Report R48369, *The United States Courts of Appeals: Background and Circuit Splits from 2024*, coordinated by Michael John Garcia (2025).

[103] *See* 4TH CIR. R. 40(e) ("Granting of rehearing or rehearing en banc vacates the previous panel judgment and opinion . . . ."); 4TH CIR. INTERNAL OPERATING P. 40.2.

[104] *Chatrie*, 136 F.4th at 100.

[105] *Id.* at 157 (Gregory, J., dissenting).

[106] *Id.* at 101, 108–09 (Diaz, C.J., concurring).

[107] *Id.* at 100 (collating alignment in front matter).

[108] *Id.* at 101 (Diaz, C.J., concurring) ("I join in affirming the district court's denial of Okello Chatrie's suppression motion, but solely on the court's finding of good faith."); *id.* at 114 (Niemeyer J., concurring) ("I also concur in the judgment of the court holding that, in any event, law enforcement's collection of the data from Google was protected because law enforcement relied in good faith on a warrant issued by a detached and neutral judicial officer."); *id.* at 115 (King, J., concurring) ("I agree that the officers acted in good faith, and I therefore also support the affirmance of the district court's judgment on that basis."); *id.* at 115 n.1 (Wynn, J., concurring) ("Although I believe that this case involved a Fourth Amendment search—and that we should say so—I acknowledge that the conditions for application of the good-faith exception to the exclusionary rule are met here."); *id.* at 143 (Heytens, J., concurring) ("And because the investigating officer could have had 'an objectively reasonable good-faith belief that [his] conduct [was] lawful,' I think the district court was right to withhold 'the harsh sanction of exclusion.'"). Between these opinions, nine judges agreed that the good faith exception applied including: Chief Judge Diaz, and Judges Niemeyer, King, Wynn, Thacker, Harris, Benjamin, Berner, and Heytens. Judge Gregory also joined Judge Wynn's concurrence, but not on the statement regarding good faith. *Id.* at 115.

[109] *Id.* at 109 (Wilkinson, J., concurring) ("With due regard for my fine colleagues, there was no search here."); *id.* at 113 (Niemeyer, J., concurring) ("Collecting markers such as these from public places or third persons is the stuff of law enforcement, enabling it to solve crimes and prosecute suspects, and the person who left them behind is not 'searched' in his person and effects, in violation of the Fourth Amendment."); *id.* at 141 (Richardson, J., concurring) ("The third-party doctrine therefore squarely governs this case.")

a reasonable expectation of privacy (at least with respect to non-anonymous data).[110] Some judges also believed that the geofence warrant itself was invalid due to a lack of probable cause.[111] One judge dissented on the ground that "the good faith exception is inapplicable in this case," and wrote that "the geofence warrant at issue glaringly infringed on the Fourth Amendment."[112]

In *United States v. Smith*,[113] the Fifth Circuit disagreed with the original Fourth Circuit panel's holding in *Chatrie*, despite ultimately affirming the district court's decision not to suppress evidence on the basis of the good faith exception. Although the Fifth Circuit acknowledged that "geofences tend to be limited temporally," it observed that "the potential intrusiveness of even a snapshot of precise location data should not be understated" given that "location tracking can easily follow an individual into areas normally considered some of the most private and intimate, particularly residences."[114] The Fifth Circuit found that, although Google Location History information requires a user to affirmatively opt in, it is still not truly voluntary due to the opacity of the opt-in process and the persistence with which "users are bombarded multiple times with requests to opt in across multiple apps."[115] The *Smith* court further analogized geofence data to the CSLI at issue in *Carpenter* and warned of "near perfect surveillance" given the pervasiveness of the underlying technology and the precision of the information.[116] However, as mentioned, *Smith* ultimately affirmed the district court's determination that suppression of the evidence in question was not warranted due to the good faith exception.[117]

Because a majority of the *en banc* court in *Chatrie* did not resolve the question of whether the collection of geofence data is a Fourth Amendment search, what had been a circuit split with the Fifth Circuit appears to have abated for now.[118] On January 16, 2026, the Supreme Court granted certiorari in *Chatrie* to consider the execution of the geofence warrant and whether it violated the

[110] *Id.* at 120–21 (Wynn, J., concurring) ("An application of the *Carpenter* factors in this case compels the conclusion that [the defendant] had a reasonable expectation of privacy in his Location History data."); *id.* at 144 (Berner, J., concurring) (distinguishing anonymized Location History data from non-anonymous Location History data and stating that "individuals do have a reasonable expectation of privacy in their non-anonymous Location History data").

[111] *Id.* at 144 (Berner, J., concurring) ("Because the Government lacked probable cause to search any specific Google user at the time it applied for the geofence warrant, this warrant was invalid and the Government's search of Chatrie violated the Fourth Amendment.").

[112] *Id.* at 157 (Gregory, J., dissenting).

[113] 110 F.4th 817 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025).

[114] *Id.* at 833.

[115] *Id.* at 835.

[116] *Id.* at 833.

[117] *Id.* at 840.

[118] Regardless, the numerous, varied opinions from the *en banc* Fourth Circuit in *Chatrie* demonstrate the ongoing legal uncertainty surrounding geofence warrants. A further illustration of the judicial disagreement may be found in *Wells v. State*, 714 S.W.3d 614, 624 (Tex. Crim. App. 2025), *reh'g denied*, No. PD-0669-23, 2025 WL 1699563 (Tex. Crim. App. June 18, 2025). There, two judges would have held that a geofence warrant did not violate the Fourth Amendment because there was no reasonable expectation of privacy in Location History due to the third-party doctrine. *Id.* at 626–27 (Finley, J., concurring). Three other judges would have held that there was no "legitimate expectation of privacy in the limited information sought through the geofence warrant's first and second steps" but that there was such an expectation "in the information sought by the warrant's third step, which included six months of prior IP history." *Id.* at 626 (Newell, J., concurring in part and dissenting in part). Further compounding the disagreement, in the opinion announcing the judgment of the court, four judges assumed that the Fourth Amendment "generally requires police to obtain a search warrant for corporate-held location history data," and the judges focused on whether the warrant was supported by probable cause and particularity, as discussed below.

Fourth Amendment.[119] The Court declined to consider a second question regarding the applicability of the exclusionary rule to evidence obtained through the geofence warrant.[120]

Table 2. The Stored Communications Act

The Fourth Amendment is not the only potential legal limit on law enforcement's ability to obtain digital information from providers. In the 1980s, decades before *Carpenter*, Congress enacted the Stored Communications Act (SCA) as part of the Electronic Communications Privacy Act (ECPA).[121] Some legislative history suggests that Congress's intent in doing so was to add supplemental protections from providers' disclosure of stored wire and electronic communications beyond those potentially contained in the Fourth Amendment. For instance, the Senate Judiciary report accompanying the ECPA described the proliferation of electronic data storage and the risk that such data "may be subject to no constitutional privacy protection" because it "is subject to control by a third party computer operator."[122] In general terms, the SCA restricts when certain information may be disclosed by Electronic Communication Services or Remote Computing Services, which in practice typically include entities such as "cell phone providers, email providers, or social media platforms" and cloud computing providers.[123] Pursuant to a provision of the SCA codified at 18 U.S.C. § 2703, the government may compel such providers to share communications' content and metadata if it obtains the requisite level of legal process, which ranges from a subpoena to a warrant, depending on the category of information sought.[124] Google has argued that, "quite apart" from the constitutional warrant requirement, § 2703(a) and (b) separately require law enforcement to obtain a warrant to compel the disclosure of Location History information.[125] It appears that some geofence warrant applications expressly invoke § 2703, and some courts have cited the statute as authorizing particular geofence warrants.[126] The limited geofence caselaw that exists, however, has primarily been resolved on Fourth Amendment grounds. Analysis of the SCA and related considerations may be found in CRS Legal Sidebar LSB10801, *Overview of Governmental Action Under the Stored Communications Act (SCA)*, by Jimmy Balser (2022).

Does a Geofence Warrant Satisfy the Requirements of the Fourth Amendment?

When the collection of geofence data is considered to constitute a search, "it follows that the government must generally obtain a warrant supported by probable cause and particularity before requesting such information."[127] Warrants may lack sufficient probable cause or particularity if they amount to a "general" warrant, which "specif[ies] only an offense, leaving to the discretion of the executing officials the decision as to which persons should be arrested and which places

[119] United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

[120] Order Granting Certiorari in Part, Chatrie v. United States, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

[121] CRS Legal Sidebar LSB10801, *Overview of Governmental Action Under the Stored Communications Act (SCA)*, by Jimmy Balser (2022).

[122] S. REP. NO. 99-541, at 3 (1986).

[123] *See* Balser, *supra* note 121.

[124] 18 U.S.C. § 2703.

[125] Brief for Google LLC as Amicus Curiae in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant at 4, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19-cr-130), 2019 WL 8227162.

[126] *E.g.*, *In re* Search of Info. that is Stored at Premises Controlled by Google, No. 2:22-MJ-01325, 2023 WL 2236493 at *5 (S.D. Tex. Feb. 14, 2023); Affidavit in Support of Search Warrant Application at 8, United States v. Smith, No. 21-CR-00107 (N.D. Miss. Feb. 10, 2023), Dkt. No. 74-2; *but cf.* Affidavit for Search Warrant, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19-CR-00130), Dkt. No. 54-1 (arguing in affidavit that there was probable cause to issue geofence warrant to Google under Virginia state law).

[127] United States v. Smith, 110 F.4th 817, 836 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025).

should be searched."[128] General warrants are "plainly unconstitutional" and their historic use in England served as a primary impetus for the Fourth Amendment.[129]

Caselaw is still developing on whether geofence warrants can satisfy Fourth Amendment particularity and probable cause requirements. The original Fourth Circuit panel in *Chatrie*, and the subsequent *en banc* court, did not reach this question (although, as noted above, several members of the *en banc* court expressed skepticism that geofence warrants could).[130] The Fifth Circuit held in *Smith* that the geofence warrant in that case amounted to a "general" warrant prohibited by the Fourth Amendment.[131] The recipient of such a warrant, the *Smith* court observed, must search "its *entire* database" to arrive at the sample of data that is actually sought by law enforcement.[132] Given that Google's review entails a search of all 592 million individual accounts with Location History enabled, the Fifth Circuit determined that it amounts to "the exact sort of general, exploratory rummaging that the Fourth Amendment was designed to prevent."[133] This review, the court held, occurs while law enforcement has "*no idea* who they are looking for, or whether the search will even turn up a result."[134] The Fifth Circuit further opined that the "quintessential problem" with geofence warrants is that they do not include sufficiently particular information, such as a specific user to be identified;[135] rather, they identify only a temporal and geographic location where a person of interest *may* turn up. Rejecting the government's claim that geofence warrants are sufficiently "limited to specified information directly tied to a particular [crime] at a particular place and time," the *Smith* court stated that, although the *results* of a geofence warrant may be sufficiently narrowly tailored as to assuage Fourth Amendment concerns, the *search* itself is not.[136] In other words, the court held that during the three-step process of reviewing, collecting, and turning over to law enforcement the requested geofence data, the warrant fails at the very first step by allowing law enforcement—albeit through Google—to "rummage through troves of location data from hundreds of millions of Google users without any description of the particular suspect or suspects to be found."[137]

A few state courts of last resort have taken a different approach than the Fifth Circuit in analyzing reverse warrants.[138] One of those cases, *People v. Seymour*,[139] which involved a keyword warrant, is discussed below.

---

[128] *Id.*

[129] *Id.*; *see also* Stanford v. Texas, 379 U.S. 476, 482 (1965) (providing historical account).

[130] United States v. Chatrie, 107 F.4th 319, 324 (4th Cir. 2024), *aff'd en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

[131] *Smith*, 110 F.4th at 824.

[132] *Id.* at 837.

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.* at 837–38.

[138] *See, e.g.*, Jones v. State, 913 S.E.2d 700, 711 (Ga. 2025) (holding that probable cause supported issuance of a geofence warrant, that the warrant was sufficiently particular, and that the first and second steps in the execution of a geofence warrant do not amount to "general rummaging"); *cf.* Wells v. State, 714 S.W.3d 614, 625 (Tex. Crim. App. 2025), *reh'g denied*, No. PD-0669-23, 2025 WL 1699563 (Tex. Crim. App. June 18, 2025) (Yeary, J., announcing judgment of the court) (assuming that a warrant was required and determining that there was probable cause for a geofence warrant and that it "provided sufficient particularity with respect to both the 'place to be searched' and the 'things to be seized.'").

[139] 536 P.3d 1260 (Colo. 2023).

Keyword Warrants

One legal scholar has characterized keyword warrants—sometimes referred to as "reverse-keyword warrants"[140]—as essentially "revers[ing]" the typical process by which law enforcement secures information about a suspect in a crime.[141] Like geofence warrants, keyword warrants begin with law enforcement identifying something they "think could be evidence"[142]—such as, in the case of geofence warrants, a location at a particular time, or in the case of keyword warrants, "a search of a particular address that was later burglarized."[143] For example, if a home located at 123 Main Street is burglarized, law enforcement may seek a keyword warrant to collect a list of search engine users who searched that address in the days prior to the burglary occurring. Law enforcement may use keyword warrants in an attempt to seek other information, too, such as the identity of users who searched for a particular person against whom a crime was later committed.

Some courts have examined the use of keyword warrants by law enforcement. In *People v. Seymour*,[144] the Colorado Supreme Court explained, "[Keyword] warrants start with a potentially incriminating piece of evidence—a search term like the address where [a crime] occurred—then request a list of users implicated by that evidence."[145] Although such warrants seek search terms rather than location data, they are still conceptually similar to geofence warrants in that neither follows the traditional process of "first identify[ing] a suspect or suspects, then obtain[ing] a warrant to search them or their property for evidence."[146]

Policies and Procedures

To date, the majority of keyword warrant cases have involved Google.[147] As is the case with geofence warrants, Google has established a process by which it responds to keyword warrants.[148] Upon receiving a keyword warrant, Google employees "formulate[] a text-based query matching the warrant's specifications" (e.g., "123 Main Street"), which is then "run against billions of daily search records from Google Search and Google Maps."[149] Google then creates a file of the matches resulting from the search and includes records that are "exact matches, or, more commonly, 'the results may extend to queries that include the specified search terms as part of a query that contains other words.'"[150] For example, if the specified search term is "123 Main Street," Google's search might return queries such as "condos at 123 Main Street" or "who lives at 123 Main Street, Springfield." Google then anonymizes the information by removing account identifiers prior to turning the file over to law enforcement, which can then review the file by categories including, for example, the actual search query, the date and time of the search, the

[140] *See supra* note 10 (discussing the terminology used to describe these types of warrants).

[141] Brian L. Owsley, *Searching a Person's Thoughts: Keyword Search Warrants and Fourth Amendment Concerns*, 28 STAN. TECH. L. REV. 66, 69 (2025).

[142] *Id.*

[143] *Id.*

[144] *Seymour*, 536 P.3d at 1260.

[145] *Id.* at 1268 n.1.

[146] United States v. Smith, 110 F.4th, 817, 822 (5th Cir. 2024); *Seymour*, 536 P.3d at 1268 n.1.

[147] *See infra* "Constitutionality of Keyword Warrants."

[148] Google reportedly "processes approximately 400 reverse-keyword warrants per year." *In re* Ct. Ord. for Prod. of Recs. to Google, LLC, No. 2024-cv-30942, 2024 WL 5314970, at *1 (Colo. Dist. Ct. Dec. 6, 2024).

[149] Owsley, *supra* note 141, at 69–70 (quoting Declaration of Nikki Adeli ¶ 4, Colorado v. Gavin Seymour, No. 21-cr-20001 (Colo. Dist. Ct. July 5, 2022) [hereinafter Adeli Decl.]).

[150] *Id.* at 70 (quoting Adeli Decl. ¶ 6).

approximate location from which the search was conducted, and the search results obtained by the user.[151] From there, law enforcement will review the anonymized data to determine which results, if any, may be relevant to their investigation (for example, law enforcement may isolate the results occurring only during a specific time frame) and exclude those that are not relevant.[152] At this stage, Google may reveal the identities of the users sought, or law enforcement may need to obtain a second search warrant if the original warrant does not authorize law enforcement to obtain identifying data.[153]

Constitutionality of Keyword Warrants

Given the novelty of keyword warrants, even less caselaw exists regarding their constitutionality than that of geofence warrants.[154] Two state court cases, however, offer what appear to be divergent views on the issue.

In *People v. Seymour*,[155] which involved a fatal residential arson, law enforcement obtained information from Google about five internet protocol (IP) addresses that were associated with devices that had searched the location of the fire in the two-week period prior.[156] To do so, law enforcement used a series of warrants to navigate Google's "staged process to respond to warrants,"[157] described above. The Colorado Supreme Court concluded that the keyword warrant amounted to a search under the Colorado State Constitution and went on to examine whether such warrants are unconstitutional general warrants.[158] The *Seymour* court rejected the defendant's contention that, because the "place to be searched" was Google's entire database, the warrant was necessarily overbroad and explained that the "ultimate touchstone" of an analysis of the legality of a warrant is "reasonableness."[159] It found the scope of the place to be searched reasonable "when we consider the filter provided by the search parameters set forth in the warrant."[160] This, the court concluded, "dramatically reduce[d] the intrusiveness of the search."[161] Of potential significance, the court discounted the idea that a warrant necessarily lacks particularity simply because of the size of the search area.[162]

---

[151] *Id.* (citing Adeli Decl. ¶ 7).

[152] *Id.* at 71 (citing Adeli Decl. ¶ 8).

[153] *Id.* (citing Adeli Decl. ¶ 9).

[154] *See* People v. Seymour, 536 P.3d 1260, 1269–70 ("The constitutionality of reverse-keyword warrants presents an issue of first impression in Colorado. Indeed, to our knowledge, no state supreme court or federal appellate court has addressed the constitutionality of such warrants."). *But see, e.g.*, *In re* Court Order for Production of Records to Google, LLC, No. 2024-cv-30942, 2024 WL 5314970 (Colo. Dist. Ct. Dec. 6, 2024) (granting in part Google's motion to quash a keyword warrant on grounds that it imposed an undue burden on the company and violated the Stored Communications Act); Owsley, *supra* note 141, at 72–73 (discussing example of a case where law enforcement may seek information using a keyword warrant); *id.* at 76 (discussing example of a case where law enforcement utilized results gathered from a keyword search warrant to identify and charge a defendant with arson outside the home of a witness in a criminal trial).

[155] 536 P.3d 1260.

[156] *Id.* at 1269.

[157] *Id.* at 1268; *see also id.* at 1268 n.1 (describing typical reverse-keyword warrant).

[158] *Id.* at 1272.

[159] *Id.* at 1275.

[160] *Id.*

[161] *Id.*

[162] *Id.* at 1275 (explaining that "'the scope of a lawful search is "defined by the object of the searches and the places in which there is probable cause to believe that it may be found"'" (quoting Maryland v. Garrison, 480 U.S. 79, 84 (continued...)

Commonwealth v. Kurtz,[163] on the other hand, involved the prosecution of an individual for rape and kidnapping.[164] Law enforcement executed a keyword warrant on Google for a report of any IP addresses that had searched the victim's address within a week of the crime.[165] This led law enforcement to the defendant who was prosecuted and who challenged the validity of the warrant on appeal.[166] The opinion[167] concluded that the "average search engine user" lacks "an expectation of privacy in the records generated" by "general, unprotected internet searches."[168] That included the defendant's Google searches for the victim's home address.[169] Therefore, the opinion did not reach the defendant's challenge that the warrant was lacking in "probable cause individualized to him."[170]

In concluding that the defendant enjoyed no reasonable expectation of privacy in his Google searches, the *Kurtz* opinion turned to *Carpenter*'s voluntariness analysis.[171] On those grounds, the opinion found Google searches as distinguishable from the cell-phone derived long-term CSLI at issue in *Carpenter*.[172] According to the opinion, a "cell phone user . . . cannot avoid creation of a data trail," but an "internet user can avoid or minimize the creation of such records by using other methods," such as making restaurant reservations in person or over the phone, conducting research through "print materials at the library," or shielding browsing history.[173] The opinion determined that every time a user "type[s] terms into a search engine and hit[s] the 'Enter' key," it represents a voluntary choice by a user to "transmit data to a third party."[174] The opinion also

(1987))). The court also emphasized that a search is not unconstitutional simply because law enforcement "cursorily examines unrelated documents," explaining that such incidental examinations are unavoidable, even in cases "when a warrant is adequately particularized," in order "'to determine whether [the unrelated documents] are, in fact, among those papers authorized to be seized.'" *Id.* at 1276 (quoting Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976)). One observer has suggested that *Seymour*, while standing for the proposition that such warrants are not per se unconstitutional, may have a potentially "limiting effect" on future uses of keyword search warrants by law enforcement, at least in Colorado, as it makes clear that law enforcement must provide sufficient particularity to justify the warrant. *See* Owsley, *supra* note 141, at 79.

[163] Nos. 98 MAP 2023, 99 MAP 2023, 100 MAP 2023, 2025 WL 3670767, at *1, 11–12 (Pa. Dec. 16, 2025), *aff'g*, 294 A.3d 509 (Pa. Super. Ct. 2023). The Superior Court in *Kurtz* also determined that the defendant enjoyed no legitimate expectation of privacy over data produced in a tower dump by AT&T. *See supra* note 52.

[164] *Id.* at *1.

[165] *Id.* at *3.

[166] *Id.*

[167] Three of the Pennsylvania Supreme Court's seven justices signed on to the Opinion Announcing the Judgment of the Court. Three justices concurred in the judgment but would not have reached the question of whether there was a search, because there was a warrant supported by probable cause. 2025 WL 3670767, at *15–19. One of those concurring justices wrote separately as well, finding that "reaching the constitutional issue" was not necessary to resolution of the appeal, but nevertheless determining that if reaching the constitutional issue were required, she would agree that "'the average search engine user' does not have 'an expectation of privacy in the records generated by unprotected internet searches.'" *Id.* at *19–20 (Mundy, J., concurring). One justice dissented. *Id.* at *20. For brevity, the Opinion Announcing the Judgment of the Court is referred to herein as the "opinion."

[168] *Id.* at *1, 11–12.

[169] *Id.* at *1.

[170] *Id.*

[171] *Id.* at *10–12; *see supra* text accompanying note 39.

[172] 2025 WL 3670767, at *10–12.

[173] *Id.*

[174] *Id.* at *10.

concluded that the terms of Google's policies further diminish a user's reasonable expectation of privacy.[175] As a result, "for purposes of federal law, the traditional third-party doctrine applies."[176]

Congressional Considerations

Courts have come to different conclusions regarding the constitutionality of reverse warrants. At minimum, a conflict continues between the Fifth Circuit in *Smith* and the Colorado Supreme Court in *Seymour* and, seemingly, amongst the *en banc* Fourth Circuit in *Chatrie*. Additional uncertainty persists given the differing views among the state courts.[177]

As discussed above, the Supreme Court granted certiorari in *Chatrie*.[178] At the time of this writing, merits briefs in the case were still forthcoming, but the petition for certiorari and the brief in opposition largely track, respectively, the opinions of the Fifth Circuit in *Smith* and the original Fourth Circuit panel in *Chatrie*. On the one hand, the defendant-petitioner argues that by requiring Google to execute a geofence warrant, the government conducted a search pursuant to *Carpenter*.[179] The defendant-petitioner also contends that the warrant violated the Fourth Amendment because it lacked sufficient particularity and was not supported by probable cause.[180] On the other hand, the government claims that the execution of the geofence warrant was not a search due to the third-party doctrine.[181] The government also disputes the defendant's claims regarding the warrant's sufficiency as to particularity and probable cause.[182]

The eventual outcome in *Chatrie* could have significant implications for geofence warrants and keyword warrants. More broadly, the case could inform the scope of *Carpenter* and the contours of the third-party doctrine in the digital age.

State legislatures have also taken an interest in reverse warrants. At least one state, Utah, has restricted the use of geofence data by law enforcement by enacting a law that generally requires investigators to obtain a search warrant for geofence data.[183] Utah has also enacted legislation restricting the use of keyword warrants.[184] Some other state legislatures have considered similar geofence and keyword warrant proposals.[185] Another approach, adopted by at least one state,[186] restricts the practice of private entities establishing geofences around health care facilities.[187]

[175] *Id.*

[176] *Id.* at *12.

[177] *See, e.g.*, discussion on opinions of the state courts of Texas and Georgia *supra* note 138.

[178] United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (mem.).

[179] Petition for Writ of Certiorari at 29, Chatrie v. United States, No. 25-112 (U.S. July 28, 2025).

[180] *Id.* at 32, 33.

[181] Brief for the United States in Opposition at 10, Chatrie v. United States, No. 25-112 (U.S. Nov. 2025).

[182] *Id.* at 11–12.

[183] UTAH CODE ANN. § 77-23f-102 (2025).

[184] *Id.* § 77-23f-102.2 (2025).

[185] *E.g.*, S.B. 49, 2025–2026 Leg. Sess. (Vt. 2025); A.B. 407/S.B. 404, 2025–2026 Leg. Sess. (N.Y. 2025); H.B. 2791, 102d Gen. Assemb., 2d Reg. Sess. (Mo. 2024); H.B. 145, 153d Gen. Assemb. (Del. 2024); A.B. 793, 2023–2024 Reg. Sess. (Cal. 2023).

[186] S.B. 49, 2025–2026 Leg. Sess. (Vt. 2025).

[187] *E.g.*, WASH. REV. CODE § 19.373.080 (2023).

At the federal level, keyword warrants have been the subject of congressional testimony.[188] Several Members of Congress also sent a letter to Google in 2022 warning of the potential use of geofence warrants in abortion investigations and asking the company to minimize its data collection practices.[189] In 2023, the Chairman of the House Judiciary Committee sent a letter to the United States Attorney General seeking information on the use of geofence warrants in January 6th investigations and in other instances.[190]

Although Congress would likely be found to have exceeded its authority in instructing the courts in how to interpret the Fourth Amendment, Congress could prohibit federal law enforcement from using reverse warrants or add additional statutory privacy protections for location information, search terms, or IP address data akin to those contained in the SCA for communications (particularly if courts ultimately reach and reject Google's position that the provisions requiring a warrant in the SCA already independently protect Location History information).[191] Alternatively, Congress may seek to codify the policies and procedures that Google has established for responding to reverse warrants, and it may codify them exactly or make the required process either more strict or more lenient. For example, Congress could require that law enforcement obtain a second warrant prior to the third step of deanonymizing the requested data, rather than relying on the initial warrant.[192]

[188] *See A Continued Pattern of Government Surveillance of U.S. Citizens: Hearing Before the H. Comm. on the Judiciary, Subcomm. on Crime and Fed. Gov. Surveillance*, 119th Cong. 7 (2025) (statement of Kia Hamadanchy, Senior Policy Counsel, ACLU) (discussing reverse warrants).

[189] Press Release, Alex Padilla, *supra* note 16.

[190] Letter from Rep. Jim Jordan, *supra* note 16.

[191] *See* Dickerson v. United States, 530 U.S. 428, 437 (2000) ("But Congress may not legislatively supersede our decisions interpreting and applying the Constitution.").

[192] As discussed above, at least one state jurisdiction seems to already require such a step. *See supra* note 86 and accompanying text.

Table 3. Select CRS Products on the Fourth Amendment, Technology, and Related Topics

- CRS Legal Sidebar LSB11274, *Geofence Warrants and the Fourth Amendment*, by Peter G. Berris and Clay Wild (2026)
- CRS Legal Sidebar LSB11339, *Advances in DNA Analysis: Fourth Amendment Implications*, by Peter G. Berris (2025)
- CRS In Focus IF13068, *Automated License Plate Readers: Background and Legal Issues*, by Peter G. Berris, Kristin Finklea, and Dave S. Sidhu (2025)
- CRS Legal Sidebar LSB11336, *Excessive Force and the Fourth Amendment: Supreme Court Clarifies Scope of Legal Test*, by Michael A. Foster and Dave S. Sidhu (2025)
- CRS Report R48160, *Law Enforcement and Technology: Use of Automated License Plate Readers*, by Kristin Finklea (2024)
- CRS Legal Sidebar LSB11165, *Disrupting Botnets: An Overview of Seizure Warrants and Other Legal Tools*, by Peter G. Berris (2024)
- CRS Legal Sidebar LSB10801, *Overview of Governmental Action Under the Stored Communications Act (SCA)*, by Jimmy Balser (2022)
- CRS Legal Sidebar LSB10786, *Abortion, Data Privacy, and Law Enforcement Access: A Legal Overview*, by Chris D. Linebaugh (2022)
- CRS Legal Sidebar LSB10713, *The Fourth Amendment and the Internet: Legal Limits on Digital Searches for Child Sexual Abuse Material (CSAM)*, by Michael A. Foster (2022)
- CRS Legal Sidebar LSB10552, *Torres v. Madrid: Police Use of Force, Fourth Amendment Seizures, and Fleeing Suspects*, by Peter G. Berris (2021)
- CRS Legal Sidebar LSB10387, *Do Warrantless Searches of Electronic Devices at the Border Violate the Fourth Amendment?*, by Hillel R. Smith (2021)

Author Information

Peter G. Berris
Legislative Attorney

Clay Wild
Legislative Attorney

Disclaimer