Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

# Geofence Warrants: A Circuit Split on Application of the Fourth Amendment

February 27, 2025

## Introduction

From thermal imaging and wiretaps to GPS tracking and various forms of electronic eavesdropping, the emergence of new technologies and their investigative use have sometimes created legal tension with constitutional privacy protections. Over the last 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. In 2024, two federal appellate courts issued diverging opinions on the constitutionality of a relatively new technology-assisted law enforcement tool—geofence warrants.

Geofences have been described as electronic systems that help establish a virtual perimeter around a specific geographic location. Private companies use geofencing for business purposes such as targeted advertising. Geofence warrants are an investigative tool typically employed when law enforcement knows the approximate time and location of a crime but not the identities of suspects. In executing a geofence warrant, law enforcement compels a company to provide certain information indicating which particular smartphones were present within a geographic area during a specified timeframe. Law enforcement can then use the information to potentially identify the owner of a smartphone found in the area of interest during the timeframe. Because geofence warrants do not begin with an identifiable suspect, they have been said to "'work in reverse' from traditional search warrants."

Law enforcement has used geofence warrants to investigate criminal matters ranging from homicides to "stolen pickup trucks and smashed car windows." The scope of geofence warrants has varied as well—from geographical areas measured in feet or meters to areas larger than an acre. Temporally, some warrants have been limited to minutes or hours; others have covered a period of days.

The use of geofence warrants has garnered media attention and legislative interest at the state and federal level. In 2023, Google announced that it would reduce the default length for which it stores the location information typically sought in geofence warrants. The move drew interest from some observers who believe it could significantly curtail the use of geofence warrants. Still, as one federal appellate court pointed out, the relevance of geofences may continue given that the government "is still seeking Google geofences," and because the government may potentially seek geofence warrants from sources other than

**Congressional Research Service**
https://crsreports.congress.gov
LSB11274

Google. Moreover, litigation over the use of geofence warrants remains ongoing, as reflected in the circuit split discussed below. This Sidebar examines evolving legal issues regarding geofence warrants and summarizes the ongoing circuit split and the various cases contributing to it—one of which was reheard *en banc* on January 30, 2025, with a decision still pending as of the time of this writing. The Sidebar concludes with considerations for Congress.

# Constitutionality of Geofence Requests

Courts have addressed two primary questions regarding the constitutionality of geofence warrants, and have not reached uniform conclusions. First, courts consider whether the collection and subsequent review of geofence data is in itself a "search" implicating the restrictions of the Fourth Amendment. Second, in the event that a court concludes that such activities do constitute a search, the court will decide if a properly issued warrant is sufficient protection under the Fourth Amendment to permit the use of geofence data in law enforcement investigations.

## Legal Background on the Fourth Amendment and Technology

In determining whether a particular means of gathering information—such as use of a geofence—constitutes a "search" triggering the protections of the Fourth Amendment, federal courts generally look to whether the government action violates a person's reasonable expectation of privacy. A variety of considerations inform 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." This concept—known as the "third-party doctrine"—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." 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. Under a broad construction of the third-party doctrine in the modern era, a potentially vast amount of digital information would exist beyond the protections of the Fourth Amendment, since such information is often shared by customers with technology providers in the ordinary course of using a product.

In an opinion that was instrumental to Fourth Amendment jurisprudence in the context of technology-assisted law enforcement, the Supreme Court in 2018 decided *Carpenter v. United States*, recognizing a limitation to the potentially expansive scope of the third-party doctrine. That case 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. 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). The *Carpenter* Court held that the CSLI was not exempt from Fourth Amendment protection pursuant to the third-party doctrine, even though the CSLI was shared by the defendant with cellular providers in the course of his cell phone use. The Court rejected the idea that the defendant's sharing of CSLI with the providers was voluntary, observing 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 in light of the fact that "a cell phone logs a cell-site record by dint of its operation." 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. This, 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 accurate and retrospective. 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.'" Nevertheless, the Court

described *Carpenter* as a "narrow" holding that did not abolish the third-party doctrine or predetermine its application to other forms of technological surveillance.

## Circuit Split: Is there a Fourth Amendment "Search" of Geofence Data?

In 2024, the U.S. Courts of Appeals for the Fourth and Fifth Circuits (Fourth Circuit and Fifth Circuit, respectively) issued diverging opinions on whether a geofence amounts to a Fourth Amendment search.

Both cases involved warrants for Google Location History. Google describes Location History as "a history or journal that [its] users can choose to create, edit, and store to record their movements and travels." Google users must agree to have their Location History monitored. Google is reportedly the primary recipient of geofence warrants. Accordingly, the procedures for executing geofence warrants, and the courts' analysis thereof as further described below, have been driven in large part by Google's corporate policies, which typically involve a three-step process. First, under that process, a warrant is obtained for an anonymized list of users in a specified geographic area and timeframe. Then, based on a review of that information and in the hopes of aiding their identification of a particular user, law enforcement can compel further contextual location information from the company for a narrower subset of users identified in step one. Finally, law enforcement may compel 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 the first two steps. What it actually means to "compel" the company beyond step one seems to vary in practice: for example, in one case a county detective in Minnesota obtained an additional warrant to compel deanonymized data from Google at the third step; but in other cases law enforcement relies on the initial search warrant to compel Google at all three steps.

In *United States v. Chatrie*, the Fourth Circuit declined to extend *Carpenter* to law enforcement's use of a warrant to collect Google's Location History information, concluding that the defendant lacked a reasonable expectation of privacy in that information (and that it therefore did not constitute a search within the meaning of the Fourth Amendment). First, the court determined that because the geofence request at issue sought only two hours of Location History, the "information obtained was therefore far less revealing" than that collected in *Carpenter* or other cases examining the bounds of the Fourth Amendment in relation to technological surveillance. Second, the Fourth Circuit said that geolocation information, unlike CSLI, is voluntarily shared because it "is off by default and can be enabled only by a user's affirmative act." Thus, the Fourth Circuit held that the third-party doctrine applied.

The Fifth Circuit disagreed with *Chatrie* in *United States v. Smith*. The *Smith* court analogized the 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. Although the Fifth Circuit conceded 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." The Fifth Circuit stated that, although Google Location History information requires a user affirmatively to opt in, it is still not truly voluntary due to the opacity of the opt-in process and its consequences and given the persistence with which users are asked to opt in. The court therefore held that the collection and review of geofence information was indeed a search under the Fourth Amendment.

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

When the use of geofence data constitutes a search, as the court in *Smith* concluded, "it follows that the government must generally obtain a warrant supported by probable cause and particularity before

requesting such information." Warrants that lack probable cause or particularity sometimes are deficient because they are "general" warrants that "specify only an offense, leaving to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." General warrants are "plainly unconstitutional" and their historic use in England served as a primary impetus for the Fourth Amendment.

The Fourth Circuit in *Chatrie* did not reach the question of whether geofence warrants satisfy Fourth Amendment requirements because it concluded that geofencing does not amount to a search and therefore does not require a warrant in the first place. By contrast, the Fifth Circuit held in *Smith* that the geofence warrant at issue amounted to a "general" warrant prohibited by the Fourth Amendment. The recipient of such a warrant, the *Smith* court observed, must search "its *entire* database" to arrive at the sample of data actually sought by law enforcement. 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." 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." The Fifth Circuit 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; rather, they only identify a time period 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 court stated that, although the *results* of a geofence warrant may be narrowly tailored as to assuage Fourth Amendment concerns, the *search* itself is not. In other words, the court held that during the review, collection, and sharing of geofence data with law enforcement, a search fails at the first step by allowing law enforcement—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."

At least one state supreme court reached a different conclusion in a case involving "reverse-keyword" warrants, which often employ procedures similar to those used in executing geofence warrants. That court held that a lawfully issued warrant can satisfy protections of the Fourth Amendment.

# Congressional Considerations

As discussed above, the Fourth and Fifth Circuits have split on whether the use of geofence data in law enforcement constitutes a search for purposes of the Fourth Amendment, and the Fourth Circuit reheard *Chatrie* en banc on January 30, 2025. In October 2024, the Department of Justice also asked the Fifth Circuit to rehear *Smith* en banc. If this circuit split persists, it could induce the Supreme Court to grant certiorari of a geofencing appeal to resolve the question. At least one practitioner has flagged geofence warrants as a topic likely to garner Supreme Court review.

A number of states have enacted laws restricting geofences in particular contexts. Many of these laws focus on banning or restricting the practice of private entities geofencing health care facilities. At least one state, Utah, has enacted a statute that generally requires investigators to obtain a search warrant for geofences or other reverse searches. At the federal level, several Members of Congress 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. 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.

Although Congress would likely exceed its authority in instructing the courts on how to interpret the Fourth Amendment, Congress could add additional statutory privacy protections for location information. For example, 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. 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. 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, although federal courts have yet to resolve that issue. Congress could amend the SCA to affect protections for location history information. Congress could also leave resolution of the legality of geofence warrants to the courts.

## Author Information

Peter G. Berris
Legislative Attorney

Clay Wild
Legislative Attorney

## Disclaimer