



Geofence Warrant Primer

Geofence warrants are a type of reverse warrant where the government seeks to know who was within a “geofence,” a defined physical area during a specific period of time. These are a type of “reverse warrant,” used to identify suspects when none are known without the data gathered by the warrant. The government utilizes geofence warrants to compel companies, such as Google, to produce information about devices interacting with their technology within a particular geographic region.

Geofence warrants are an unprecedented increase in the government’s ability to locate individuals without substantial investigation or investment of resources. Through geofence warrants, the government can obtain what Google refers to as “Location History” data. Location History keeps records about where a user’s device is at any given time through a variety of data, including: GPS information, Blue-tooth beacons, cell phone location information from nearby cell towers, Internet Protocol address information, and the signal strength of nearby WiFi networks. *United States v. Chatrie*, 2022 WL 628905, *3 (E.D. Va. Mar. 3, 2022). For a more in depth discussion of Location History and the differences from CSLI, please see NACDL’s Geofence webinar.

¹Geofence warrants are general warrants—which are prohibited by the Fourth Amendment—because they are devoid of probable cause and particularity. To suppress evidence from a geofence warrant, it is necessary to demonstrate a Fourth Amendment search occurred, the search violated the constitution, and the good faith exception does not apply.

Steps in the Geofence Process

The geofence process involves up to three steps, which may be completed through a single or multiple warrants or through a combination of warrants and other forms of process.

Step One: The government first seeks anonymized numerical identifiers and time-stamped location coordinates for every device that passed through an area in a specified window of time. This information is obtained from a company, most commonly Google, using a geofence warrant. The data provided to law enforcement in Step One is not truly anonymized because people can be easily identified from their Location History data, and the government can get subscriber information for anonymous IDs with only a subpoena after Step One. See *Chatrie*, 2022 WL 628905 at *22 n.39 (noting that the collection of “anonymized location data” through a geofence warrant “can reveal astonishing glimpses into individuals’ private lives”).

Step Two: The government reviews the list and culls it using other investigative techniques. Sometimes the government requests more information about particular accounts from the company. That request may be made by a private letter to the company for more location history for a longer period of time with no geographic limitations.

Step Three: The government further narrows the list and requests identifying information (e.g., usernames, birth dates, and other identifying information of the phones’ owners) from the company for the culled list of users through the initial warrant or an additional warrant, court order, or subpoena.

Was There a Fourth Amendment Search?

To establish there was a search, first argue there is a reasonable expectation of privacy under *Carpenter v. United States*, 138 S. Ct. 2207, 2217 (2018). Under *Carpenter’s* test, users have a reasonable expectation of privacy in their Google Location History.

First, Location History has “depth, breadth, and comprehensive reach” similar to the cell site location information (“CSLI”) at issue in *Carpenter*, and allows the government to historically reconstruct an individual’s past movements in a way that would have been impossible at the time of the adoption of the Fourth Amendment. 138 S. Ct. at 2223; see also *Leaders of a Beautiful Struggle v. Baltimore*, 2 F.4th 330, 334 (4th Cir. 2021) (holding “*Carpenter* squarely applie[d]” when images in a location tracking scheme allowed law enforcement to “travel back in time” as if they had “attached an ankle monitor” to every person in the city). In an amicus brief in one geofence warrant case, Google stated that Location History “can often reveal a user’s location and movements with a much higher degree of precision than [CSLI].” *Chatrie*, 2022 WL 628905 at *2 n.5.

Second, Location History is sensitive and reveals the “privacies of life.” *Carpenter*, 138 S. Ct. at 2214. Geofence warrants request information on all devices within a virtual perimeter defined by law enforcement from large technology companies like Google with the hope of identifying a suspect amongst innumerable people. Depending on the boundaries of the geofence, the data may locate cell phones or other devices within “private residences, doctor’s offices, political headquarters, and other potentially revealing locales,” *Carpenter*, 138 S. Ct. at 2218; see also *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (stating that courts should carefully consider the “power of technology to shrink the realm of guaranteed privacy”). This invasion of constitutionally protected spaces is “presumptively unreasonable in the absence of a search warrant.” *Katz v. United States*, 389 U.S. 347, 361 (1967).

Finally, the third-party doctrine does not apply because Location History, like CSLI, is distinct from “the limited types of personal information addressed in *Smith and Miller*.” *Carpenter*, 138 S. Ct. at 2219. Google account holders cannot voluntarily share their location information in a meaningful way because a regular person would not be able to understand the frequency nor the precision of Google’s location track-ing. See *Chatrie*, 2022 WL 628905 at *26.

Users also have a possessory interest in their Location History data. Google treats Location History as user property that it holds in trust. See *Chatrie*, 2022 WL 628905 at *2 n.5 (“Location History is not a business record, but is a journal stored primarily for the user’s benefit and is controlled by the user.”). The right to total exclusion of others from one’s property is “one of the most treasured strands” of the property rights bundle. *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982). The government’s acquisition of a user’s Location History constitutes a search under a traditional approach to the Fourth Amendment.

Was There a Constitutional Warrant?

The Fourth Amendment requires a warrant (1) be supported by probable cause; (2) particularly describe the place to be searched and the things to be seized; and (3) be issued by a neutral disinterested magistrate. *Dalia v. United States*, 441 U.S. 238, 255 (1979) (cleaned up). If a geofence warrant fails even one these requirements it is unconstitutional, and if a warrant is invalid, the appropriate remedy is to sup-press the evidence derived from it. *United States v. Calandra*, 414 U.S. 338, 347 (1974).

Geofence warrants implicate the First Amendment because location information can expose a person’s speech or “familial, political, professional, religious, and sexual associations.” See *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Courts must apply Fourth Amendment requirements to geofence war-rants with “the most scrupulous exactitude” when they implicate First Amendment concerns. *Stanford*, 379 U.S. at 485.



Was the Search Overbroad?

By design, geofence warrants do not specify the person or people whose Google accounts will be searched. Instead, the goal is to search across “numerous tens of millions” of user accounts and then identify specific accounts that law enforcement would like to search further. Decl. of Marlo McGriff ¶ 13, *Chatrie*, No. 3:10-cr-130-MHL (E.D. Va. (Mar. 11, 2020), ECF No. 96-1). The scope of geofence warrants is intentionally overbroad. However, to be constitutional, the scope of a search must be tailored to the probable cause in each case.

Probable cause is “a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983). But, the fact that users caught in a geofence warrant were close to the site of an alleged crime does not, without more, give rise to probable cause to search that person. See *Ybarra v. Illinois*, 444 U.S. 85, 91.

Similarly, the fact that an alleged crime occurred does not support probable cause to search many or any unidentified people. In *Chatrie*, the court found “unpersuasive the United States’ inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person nearby.” *Chatrie*, 2022 WL 628905 at *24. Geofence warrants are overbroad searches without sufficient, or any, probable cause.

Was the Search Particularized?

Geofence warrants permit law enforcement and Google to exercise an impermissible amount of discretion during Fourth Amendment searches and seizures.

In Step 1 of a geofence warrant, the government does not particularly describe what will be searched or seized, instead leaving both determinations to Google’s discretion. A geofence warrant generally requires Google to search “all location data.” It does not particularly describe what data Google must search (e.g., Location History data versus Web & App Activity data versus Google Location Accuracy data) based on probable cause. Also, a geofence warrant does not particularly describe the things to be seized. Instead, it leaves to Google’s discretion how to “count” which users fall within a geofence, without providing necessary probable cause for those users. This falls short of the particularity requirement because “a person’s mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.” *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979).

In Step 2 and 3 of a geofence warrant, law enforcement seeks and Google provides additional, deanonymizing information about users without justifying their choices to a judge. In *Chatrie*, the court implied that to satisfy particularity a geofence warrant must leave “ultimate discretion as to which users’ information [is disclosed] to the reviewing court, not to Google or law enforcement.” *Chatrie*, 2022 WL 628905, at *23. The court emphasized that constitutional warrants must incorporate “a court’s authorization” when law enforcement successively seeks information about specific users, not authorization from a third party. *Chatrie*, at *24.

Did the Government Act in Good Faith?

The good-faith exception is limited to when law enforcement acts in good faith reliance on a warrant that is later found to be unconstitutional. *United States v. Leon*, 468 U.S. 897, 922 (1984). Note, some jurisdictions do not have the good faith exception, while others have additional factors in the inquiry. Ultimately, good faith requires a very fact-dependent argument.

Due to the glaring deficiencies of geofence warrants as a category—the absence of probable cause for all individuals searched, the overbreadth, and the lack of particularity for what is searched and seized—law enforcement cannot have an “objectively reasonable reliance” on geofence warrants. *Leon*, at 922. Furthermore, the good faith exception to the exclusionary rule is inapplicable because so much of the evidence that is collected through geofence warrants is particularized behind closed doors and without judicial approval.



Discovery and Subpoena Material

You will need to get information from both the government and Google to successfully litigate a motion to suppress. NACDL has several resources available for reference:

- [Geofence Discovery Motion](#) from *United States v. Chatrie* ²
- [Motion to Suppress](#) from *United States v. Chatrie* ³
- [Order Granting Defense Request for Subpoena to Google](#) ⁴
- More resources can be found on [NACDL's website](#) ⁵

Case List

- *Carpenter v. United States*, 138 S. Ct. 2206 (2018)
- *United States v. Di Re*, 332 U.S. 581 (1948)
- *Katz v. United States*, 389 U.S. 347 (1967)
- *Kyllo v. United States*, 533 U.S. 27 (2001)
- *Leaders of a Beautiful Struggle v. Baltimore*, 2 F.4th 330 (4th Cir. 2021)
- *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419 (1982)
- *Smith v. Maryland*, 442 U.S. 735 (1979)
- *United States v. Chatrie*, 2022 WL 628905 (E.D. Va. Mar. 3, 2022)
- *United States v. Miller*, 425 U.S. 435 (1976)
- *Dalia v. United States*, 441 U.S. 238 (1979)
- *Illinois v. Gates*, 462 U.S. 213 (1983)
- *In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, (N.D. Ill. 2020)
- *Riley v. California*, 573 U.S. 373 (2014)
- *Steagald v. United States*, 451 U.S. 204 (1981)
- *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam)
- *United States v. Galpin*, 720 F.3d 436 (2d Cir. 2013)
- *United States v. Leon*, 468 U.S. 897 (1984)
- *Ybarra v. Illinois*, 444 U.S. 85 (1979)
- *NAACP v. Alabama*, 357 U.S. 449 (1958)
- *Stanford v. Texas*, 379 U.S. 476 (1965)
- *United States v. Jones*, 565 U.S. 400 (2012)

Additional Resources

- Thomas Brewster, "[Feds Order Google to Hand Over a Load of Innocent Americans' Locations](#)," *Forbes* (Oct. 23, 2018)
- Tyler Dukes, "[To Find Suspects, Police Quietly Turn to Google](#)," *WRAL* (Mar. 15, 2018)
- Jennifer S. Granick, "[Making Warrants Great Again: Avoiding General Searches in the Execution of Warrants for Electronic Data](#)" (Dec. 2021)
- Michael Price & Bill Wolf, "[Building on Carpenter: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider](#)" (Dec. 2018)
- Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181 (2016)
- Google, [Privacy Policy, Information Google Collects: Your location information](#) (2022)

NACDL Resources

- [United States v. Chatrie Content Page](#)
- [Digital Location Tracking Content Page](#)
- [Reverse Search Warrant Content Page](#)

Editor's Note: The content pages listed above can be found at [nacdl.org](#). In addition, NACDL's webinars on geofences, location privacy after Carpenter, and the third-party doctrine and location tracking can be found by visiting <https://www.nacdl.org/Content/Fourth-Amendment-Center-Videos>.



NACDL FOURTH
AMENDMENT CENTER

For litigation assistance and other resources contact 4AC@nacdl.org

Notes

1 <https://www.nacdl.org/Content/When-Google-Searches-for-You-Challenging-Geofence>

2 <https://www.nacdl.org/getattachment/0d3728fa-24b0-4df5-929a-9ccaef71c0fb/189110047428.pdf>

3 <https://www.nacdl.org/getattachment/a16a7368-3691-4b32-b479-ad8128c53016/5f0ba578-cfe1-4fb9-9e76-5d40778f3f40.pdf>

4 <https://www.nacdl.org/getattachment/19831ec4-9272-4072-ae89-d5bf4827235d/order-granting-defendant-s-motion-for-issuance-of-subpoena-duces-tecum.pdf>

5 <https://www.nacdl.org/Landing/Resource-Center>