

Geofence Warrants and the Fourth Amendment

Kelly Adams

A geofence warrant is the information that the government compels from large data companies, such as Google, that provides information about who was present in a given area at a specified time.¹ This data about mobile devices in certain areas is often in an anonymized form, but it can be identified without much difficulty.² This raises serious constitutional concerns surrounding the Fourth Amendment and warrants. This blog will go further in depth about what a geofence warrant is, how it might be an unconstitutional search, and how it might be unconstitutional for warrant purposes.

Geofence warrants work differently than traditional warrants. They are often used when law enforcement knows the general time and location of a crime, but not who was present in that area.³ They compel companies (most often, Google)⁴ to provide information about devices that were present in the area at the time.⁵ These warrants vary in their scope as it relates to both time and geographic area.

Geofence warrants are unique. For one, they don't require law enforcement to single out a specific person or suspect when they seek a warrant.⁶ Instead, law enforcement can get information about every person in that area. Though they are not well-known, these warrants have been used in response to significant events, including the January 6th, 2021 insurrection at the Capitol, protests in Minneapolis following the murder of George Floyd, and protests in Kenosha Wisconsin after the murder of Jacob Blake.⁷ Another reason that this is such a unique process is because the data is often anonymized when received.⁸ This is not a significant barrier because the data can easily be identified, and the government can request subscriber information with a subpoena.⁹ The government may also request more data from companies about various accounts.¹⁰

Geofence warrants raise Fourth Amendment search issues for numerous reasons. To start, there is the issue of whether there is a reasonable expectation of privacy in the data sought in the warrant. Because of how precise and invasive these warrants can be, many argue that there is a Fourth Amendment violation here.¹¹ However, a district court in Virginia held that they did not need to decide the issue of whether there was a reasonable expectation of privacy with this data.¹²

¹ *Geofence Warrant Primer*, NAT'L ASS'N OF CRIM. DEF. LAW. 1, 1 <https://www.nacdl.org/getattachment/816437c7-8943-425c-9b3b-4faf7da24bba/nacdl-geofence-primer.pdf> [<https://perma.cc/8SBX-MGSB>].

² *Id.*

³ *Geofence Warrants: A Circuit Split on Application of the Fourth Amendment*, CONG. RSCH. SERV. 1, 1 (Feb. 27, 2025), <https://www.congress.gov/crs-product/LSB11274> [<https://perma.cc/5J34-YDYF>].

⁴ *Id.* at 3.

⁵ *Id.* at 1.

⁶ *Id.*

⁷ Navdeep Kaur Bal, *The Constitutionality of Geofence Warrants*, BERKELEY J. OF CRIM. L. BLOG (Jan. 18, 2024), <https://www.bjcl.org/blog/the-constitutionality-of-geofence-warrants> [<https://perma.cc/BH7Y-UY43>].

⁸ *Geofence Warrant Primer*, *supra* note 1 at 1.

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.* at 2.

¹² Bal, *supra* note 7.

This has created a divide, because some people argue that users can opt out of location services and avoid this problem.¹³ Others counter that it might not be so easy, and that devices are collecting location data constantly.¹⁴

Geofence warrants also raise concerns about overbroad searches in violation of the Fourth Amendment. The Fourth Amendment requires that warrants should be supported by probable cause, they should describe the place to be searched and the things to be seized with particularity, and they should be issued by a neutral magistrate.¹⁵ Geofence warrants don't specify the data sought in the same way that the average warrant does. Instead, geofence warrants have an incredibly broad scope, and they access data from thousands of people in a given area.¹⁶ The warrant generally demands "all location data" without giving the companies a more specific description.¹⁷ When the government isn't required to narrow their search, this can raise serious constitutional issues.

The reach of geofence warrants arguably resembles "general" warrants. A general warrant is one that only specifies an offense, which leaves law enforcement with the power to determine who should be arrested and where to search.¹⁸ These warrants are unconstitutional and are one of the injustices that the Fourth Amendment was made to protect against.¹⁹ Geofence warrants, by not specifying a distinct suspect, resemble these unconstitutional warrants.

The breadth of a search must relate to probable cause.²⁰ Geofence warrants are typically justified because law enforcement will provide probable cause for searching that area. However, just because a crime happened in a specific location does not create probable cause for searching so many unidentified individuals.²¹ Once the government determines someone's presence in a certain area at the given time, further warrants are necessary to perform a physical search on that individual.²²

Courts are split on the constitutionality of geofence warrants. In *United States v. Chatrie*, the Fourth Circuit determined that requesting information for a span of two hours was permissible and did not violate the Fourth Amendment. The Fourth Circuit also said that geolocation information is given voluntarily by individuals, because the default is to not collect information, and it must be turned on in the app's settings.²³

However, in *United States v. Smith*, the Fifth Circuit highlighted the invasive quality of geofence warrants, and how they pose a serious threat to privacy and the Fourth Amendment. The Fifth Circuit addressed the matter of opting in that the Fourth Circuit discussed. They determined

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Geofence Warrant Primer*, *supra* note 1 at 2.

¹⁶ *Id.*

¹⁷ *Id.* at 3.

¹⁸ CONG. RSCH. SERV., *supra* note 3 at 4.

¹⁹ *Id.* at 4.

²⁰ *Geofence Warrant Primer*, *supra* note 1 at 2.

²¹ *Id.*

²² *Id.*

²³ CONG. RSCH. SERV., *supra* note 3 at 3.

that opting in may not be completely voluntary because the process of opting in is misleading and users are repeatedly asked to do so.²⁴ The Fifth Circuit held that “collection and review of geofence information was indeed a search under the Fourth Amendment.”²⁵

Geofence warrants indicate that technological surveillance is spreading in our society and is being utilized by law enforcement. As we experience rapid change, it is important to understand the constitutionality of law enforcement’s actions. Geofence warrants raise serious Fourth Amendment concerns because of overbreadth and the reasonable expectation of privacy. Courts are split on how to address this issue; some are more cautious about the dubious constitutionality of geofence warrants while others emphasize the voluntary choice for users to opt in to data collection by Google and other big companies. The future of these warrants is unclear, as there are likely more decisions to come in American courts.

²⁴*Id.*

²⁵ *Id.*