LIBERTAS INSTITUTE

**Primary Office**
2183 W Main St, #A102
Lehi, Utah 84043
(801) 901-0310

**Policy Memo**

# Geofence "Warrants": An Unconstitutional Abuse of Technology

General warrants give law enforcement agents broad authority "to search and seize unspecified places or persons."[1] Prior to the American Revolution, this type of search—known as a writ of assistance—was widely used by British officials to search colonists' imported goods to ensure compliance with the tax code.[2] James Otis, a young lawyer from Boston, gave an impassioned defense of civil liberties and struck a chord with colonists. In an 1817 letter to William Tudor, John Adams referred to Otis's speech as the birth of America's struggle for independence.[3]

Today, the Fourth Amendment protects Americans from the unreasonable searches and seizures of a time gone by. However, technological advances have brought general warrants into the modern era in the form of geofence warrants.

Geofence warrants are reverse searches used by law enforcement to identify suspects in criminal investigations. These searches take advantage of modern technology by identifying all users present within a virtually bounded geographic area. Just like the broad writs of assistance from the colonial era, these warrants give law enforcement the broad authority to search unspecified persons before they are implicated in the crime being investigated.

Currently, Google receives nearly all of these types of warrant requests. The corporation's extensive location history database—one that is notoriously difficult to opt out of—has understandably caught the eye of law enforcement agents who have quickly seen the investigative power of a database containing a history of a vast swath of the public's physical movements.

To assess the use of these warrants within the state of Utah, Libertas reviewed forty geofence warrants issued in Salt Lake County, Weber County, Davis County, and Layton County between January 2016 and December 2021.

The reviewed warrants included requests seeking cell site location information, i.e. data collected from cell phone "pings" on towers in a discrete geographic area at a specific time, and requests sent to Google seeking customer data derived from Google's database of location history.

These warrants give law enforcement the broad authority to search unspecified persons before they are implicated in the crime being investigated.

[1] "General Warrant Law and Legal Definition," USLegal, https://definitions.uslegal.com/g/general-warrant/.

[2] Tim O'Brien, "Suspicionless Search: Geofence Warrants and the Fourth Amendment," SSRN, August 5, 2021, page 5, https://ssrn.com/abstract=3834623

[3] "From John Adams to William Tudor, Sr., 29 March 1817," U.S. National Archives, https://founders.archives.gov/documents/Adams/99-02-02-6735.

All the reviewed warrants allowed law enforcement to retroactively sift through the data that was available or accessible within a “fenced” area. Additionally, searches routinely requested an order from the court barring Google from disclosing the existence of the search, leaving users subject to searches unaware that law enforcement was sifting through their data.

Our research identified three types of warrants: (1) searches requesting data from cell towers servicing a specific location, on a certain day, for a set period of time (generally a few hours); (2) searches requesting data that “pinged” to a tower within a specific radius (e.g., a few hundred meters); and (3) searches requesting data from the Google Reverse Location database. This type of warrant does not list a specific physical area for the search, instead relying on Google’s ID numbers to serve as digital markers.

These three types of searches may be combined by law enforcement. For instance, searches requesting information connected to specific Google ID numbers relied on information obtained from a prior geofence search. Additionally, searches are not necessarily limited to one “fenced” location, and fenced areas are often drawn broadly enough to include busy metropolitan areas where there is near constant cell phone traffic.

Although it is well known that law enforcement seeks initial, anonymized data dumps from companies such as Google, geofence warrants *are used* to request personal information about customers that go beyond physical location.[4]

Our research confirms Utah law enforcement anticipates unmasking users. Searches vary in the degree of information requested, but a warrant issued on December 1, 2021, shows how broad requests may be.[5] For example, a warrant issued in Davis County anticipated an unmasking process, stating that after law enforcement analyzed the initial data provided by Google, “further legal process” would be utilized to identify users near the scene of the crime.

**Constitutional Concerns**

The text of the Fourth Amendment reads as follows:

> *“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.”*

The amendment uses a two-pronged approach to assess the validity of warrants. First, warrants must be predicated on **probable cause**. Second, warrants must describe with **particularity** the place to be searched and the person or things to be seized.

Geofence reverse search warrants reviewed by Libertas fail to meet these constitutional requirements.

---

[4] NOTE: Against Geofences, 74 Stan. L. Rev. 385, 400.

[5] See Warrant Spreadsheet compiled by Libertas Institute at TinyURL.com/geofencewarrant

*1. Probable Cause*

Constitutionally speaking, probable cause exists when there is a "a fair probability that contraband or evidence of a crime will be found in a particular place."[6] In the context of geofence warrants, the relevant question to answer is whether geofence warrants are predicated on a reasonable belief that evidence of a crime will be found within the fenced area.

Initially, geofence warrants seek anonymized data that speaks to no fact other than the physical location of Google users. This information is neither contraband, which is anything that is illegal to possess, nor is physical location evidence of criminal activity.[7]

In the case of *Ybarra v Illinois*, law enforcement executed a warrant obtained to search a tavern expecting to find evidence of the illicit drug heroin. However, the warrant did not specify a search of Ventura Ybarra. Following his grand jury indictment for the crime of unlawful possession of a controlled substance, Ybarra filed a motion to suppress evidence of the contraband at trial.

Eventually his case was heard by the Supreme Court who determined law enforcement violated the Fourth Amendment because "a person's mere propinquity to others suspected of criminal activity does not, without more, give probable cause to search that person."[8]

Probable cause, then, cannot be based on geographic location alone. Consequently, law enforcement cannot use knowledge that a crime was committed in location A to establish the constitutionality of searching all users in location A, particularly when most users are known to be innocent at the time of the search.

Yet by their nature, geofence warrants seek to search individual users based on nothing but the coordinate points provided to Google. This defect in the searches has led some judges to invalidate warrant affidavits.

For example, Magistrate Judge Mitchell in Kansas denied a geofence warrant affidavit because although there was probable cause establishing the commission of a crime within the virtually bound geographic region, the government was unable to show evidence of that crime would be located in Google's records.[9]

*2. Particularity*

The particularity requirement of the Fourth Amendment states warrants are invalid unless they "particularly [describe] the place to be searched, and the persons or things to be seized."

---

[6] Illinois v. Gates, 462 U.S. 213, 216, 103 S. Ct. 2317, 2320, 76 L. Ed. 2d 527, 534, 1983 U.S. LEXIS 54, *5, 51 U.S.L.W. 4709.

[7] "Contraband," Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/wex/contraband.

[8] Ybarra v. Ill., 444 U.S. 85, 91, 100 S. Ct. 338, 342, 62 L. Ed. 2d 238, 245, 1979 U.S. LEXIS 151, *12

[9] NOTE: Against Geofences, 74 Stan. L. Rev. 385, 445.

Geofence searches violate this requirement because, due to their inherent breadth, they are unable to particularly describe the things to be seized. Requesting all user information within a specific geographic location is, definitionally speaking, the opposite of particular or specific.

In an opinion from the Northern District of Illinois, Magistrate Judge Weisman attacked the validity of a geofence warrant brought before him, stating “no objective measure that limits the agents' discretion in obtaining information as to each cellular telephone in the geofence.”[10]

Judge Weisman undercut a common argument employed by law enforcement. This argument analogizes geofence warrants to an investigative tool used by the FBI to identify users on Playpen, a site used for uploading and downloading child pornography.[11]

Playpen is not generally discoverable on the open web and does not populate through standard Google search, giving law enforcement reasons to believe any user accessing the website is breaking the law. Furthermore, the site’s purpose gives law enforcement sufficient knowledge to narrow down the contents of their search, i.e., the contraband that is child pornography.[12]

Unlike the circumstances in the Playpen case, geofence warrants seeking all location data from users within a set geographic boundary is not sufficiently narrow. Unlike Playpen, users within a geofenced area are not accessing the space for the purpose of engaging in illegal activity. Additionally, the information law enforcement seeks to seize has no limitation and is based solely on the agent’s judgment.[13]

**Legislative Reforms Needed**

Given the breadth of Google’s location history database, inaccessibility of halting all collection of location information, and the reality that most Americans are incapable of preventing routine searches of their physical movements, fertile ground has been created for mistrust between police and the population they serve.

Fertile ground has been created for mistrust between police and the population they serve.

Even Google employees remain uncertain of how to prevent their employers from obtaining their physical location. One employee noted that Google’s messaging surrounding the disablement of location history on a device was so confusing that a “privacy focused [software engineer]” would find it difficult to determine with certainty how to prevent the corporation from tracking his or her physical movements.[14]

While all searches that evade Fourth Amendment requirements and the rule of law should be rejected, the scope of the problems with geofence warrants are systemic and broad. Law enforcement has

---

[10] In re Search of Info. Stored at Premises Controlled by Google, 2020 U.S. Dist. LEXIS 165185, *14, 2020 WL 5491763.

[11] Ibid., 15.

[12] Ibid.

[13] Ibid.

[14] NOTE: Against Geofences, 74 Stan. L. Rev. 385, 397.

been moving quickly to capitalize on the widespread use of Google location history using dragnet searches to identify suspects in a variety of criminal investigations.[15]

The problem becomes more thorny once the error rate of geofence warrants is factored into the equation. Despite only a 68 percent accuracy rate, the use of geofence warrants has skyrocketed in recent years. In 2019, Google's transparency report showed a year over year increase of 1,500 percent in the number of requests received in 2018 compared to 2017.[16] Given that this does not include the past four years of data, it stands to reason the use of these warrants has only increased with time.

Utah is not the only state contending with this problem. John C. Ellis, Jr, a digital forensic consultant and expert, updated his primer on Google's location data collection practices and the process used by law enforcement to access the corporation's extensive databases. The three-step process he describes starts with an anonymized data dump and ends with an unmasking process.

This process corresponds to the search warrants issued in Utah reviewed by Libertas. As Tim O'Brien notes in his article, the initial "anonymization" language used by law enforcement to secure these search warrants is a fallacy because the entire purpose of the first warrant is to secure information that will inevitably lead to the unmasking of users.[17]

Although some judges are quick to note the constitutional defects of geofence warrants, others are not. The exponential increase in the issuance of these warrants underscores a harsh reality—the judiciary is not prepared to address the problems with these warrants in a timely fashion.

This is unsurprising since until recently geofence warrants were novel and rarely used. The database from which law enforcement obtains initial data dumps was originally intended for the purpose of targeted marketing.[18] It was not until a cold case in North Carolina was solved in 2017 that the new investigative tool took off.[19]

Legislators should ensure Utahns are protected in a manner consistent with the Fourth Amendment by clarifying the use of geofence warrants. As with any investigative tool, law enforcement should be required to show probable cause and particularity prior to obtaining a search warrant.

Kansas Judge Angel Mitchell focused her analysis of the validity of geofence warrants on the breadth of the search and its relation to the underlying investigation. Statutory reforms should have a similar focus, ensuring there is particularity and probable cause—which is the constitutional standard for warrants anyway—before being issued.

---

[15] See Warrant Spreadsheet showing crimes investigated using geofence warrants range in severity from property and low-level theft to more serious violent crimes.

[16] O'Brien, "Suspicionless Search," 19.

[17] Ibid.

[18] Ibid., 3.

[19] Ibid., 1.