SAMUELSON-GLUSHKO TECHNOLOGY LAW &

POLICY CLINIC

GEOFENCE WARRANTS: A MODEL STATE POLICY

UNIVERSITY OF COLORADO LAW SCHOOL

This report was written by Vivek Krishnamurthy, Sarah Baldwin, Zoe Leonore Glepa, and Victor Laudano of the Samuelson-Glushko Technology Law & Policy Clinic (TLPC).

Based at the University of Colorado Law School, TLPC advocates for technology laws and policies that advance the public interest at the international, national, and local levels. The Clinic addresses a wide range of issues, from civil and human rights to privacy and intellectual property law. TLPC engages in discussions on technology law and policy by representing clients before administrative, judicial, and legislative bodies, participating in amicus advocacy, conducting significant public policy research, and forming strategic partnerships with advocacy groups, public officials, and multistakeholder groups to effect change. For more information, visit our website at https://tlpc.colorado.edu/.

The authors are grateful to Jake Laperruque, Deputy Director of the Security and Surveillance Project at the Center for Democracy and Technology, for his tireless support of his project; to Erin Calkins, the Communications Coordinator at the University of Colorado Law Clinics, for her work in preparing this report for publication; and to all of our 2024-25 TLPC student attorneys for their help in workshopping the ideas contained in this report. Any remaining errors are those of the authors alone.

Published June 2025 using the tufte-book class in LaTeX.

Contents

Introduction

Law enforcement is increasingly using geofence warrants—court orders that compel companies to turn over location data for devices within a specified area and timeframe—to aid in criminal investigations. While geofence warrants can be valuable tools, they raise significant concerns about privacy and the potential for misuse.

Although various courts have grappled with the use of geofence warrants in law enforcement investigations, no clear consensus has emerged. Some courts view geofence warrants as inherently unconstitutional, while others argue that they do not constitute searches under the Fourth Amendment.

Legislators cannot wait for the courts to define the boundaries through case law; proactive legislation is needed to establish clear and enforceable guidelines. To that end, the Samuelson-Glushko Technology Law and Policy Clinic (TLPC) at the University of Colorado Law School has developed a model policy framework to govern the use of geofence warrants. We have done so at the request of the Center for Democracy & Technology (CDT), a leading nonpartisan, nonprofit organization fighting to advance civil rights and civil liberties in the digital age. Although TLPC consulted with CDT while developing this policy, the views expressed in this document are solely those of the TLPC staff members who created it and do not represent the views of CDT.

Our model policy provides a comprehensive framework to address concerns surrounding geofence warrants. It seeks to strike a balance between the vital need to safeguard civil liberties and the legitimate use of geofence warrants as an investigative tool of last resort.

This proposal presents a set of policy recommendations designed to clarify the conditions under which geofence warrants may be issued. It provides a framework to ensure they are used subject to strict judicial scrutiny and oversight. The proposed policy sets threshold requirements that law enforcement must meet before requesting a geofence warrant, helping ensure such warrants are used only when they are strictly necessary. We also recommend applying specific tailoring factors—such as limiting the geographic area and timeframe

covered—to minimize unnecessary privacy intrusions caused by using such warrants.

To further safeguard individual rights, our proposal requires law enforcement to demonstrate a clear and specific need for a geofence warrant at every stage of the process. By imposing progressively higher standards of proof as the potential impact on privacy increases, the policy aims to strike a careful balance between effective investigative tools and robust privacy protections.

We also recommend incorporating supplemental procedures—such as a notification requirement—to promote transparency and accountability in the collection and use of location data. This is especially important in today's rapidly evolving location data ecosystem, where advances in technology and growing device interconnectivity continuously reshape how personal and location-based information is collected, shared, and used. Implementing these measures will help protect individual privacy and foster greater public trust in the digital environment.

This policy proposal begins by explaining how location data is collected and stored, and how law enforcement agencies have sought access to such data from the companies that collect it. It then evaluates the current legal framework for evaluating geofence warrant applications and explores the rapidly evolving technological landscape surrounding location data. We then review the scholarship on geofence warrants to highlight key concerns associated with their use. Building on this foundation, we offer policy recommendations for lawmakers to consider in regulating geofence warrants. By establishing clear and enforceable guidelines, our proposal aims to balance the investigative utility of geofence warrants with the imperative to protect individuals' digital privacy.

Background

Understanding Location Data

Understanding location data is essential to understanding geofence warrants. Location data reveals where a device is situated in the world and is generated through technologies such as Global Positioning System (GPS), Wi-Fi, cell tower triangulation, or a combination of these methods. The precision of location data varies: some sources provide highly accurate information, while others offer only approximate locations. GPS-enabled smartphones typically generate the most precise data, often accurate within a five-meter radius (16 feet).[1] In contrast, cell-site location information can be less reliable, with accuracy influenced by factors such as signal strength, tower density, and network load.[2] Wi-Fi-based location data, which estimates a device's position based on signal strength from nearby routers, can also vary in accuracy depending on the environment.[3]

Regardless of the method, these technologies enable a range of entities in the contemporary digital ecosystem to collect, store, and use location data and leverage location-based insights in real time. Location data is frequently collected through social media apps (such as Facebook or Instagram), navigation apps (like Google Maps or Waze), and gaming apps (such as Pokémon Go!).

While many apps and digital services gather location data with the formal legal permission of their users, such permission is neither informed nor meaningful in practically all circumstances. Most users of digital services have neither the time nor the ability to read terms of service before accepting them. Indeed, it would take the average American 76 days to read the terms of service they encounter in the average year.[4] Moreover, the consequence of saying "no" to services that collect location data is to cut oneself off from services that are essential to our ability to function in an increasingly digitized society.

Technology companies, retailers, and data brokers all play a role in handling location data—but the role of data brokers is particularly concerning. Unlike other entities, data brokers do not merely collect data; they aggregate and sell it to third parties, including law

[1] GPS Accuracy, GPS.gov, https://www.gps.gov/systems/gps/performance/accuracy (last visited Apr. 11, 2025).

[2] Jay Stanley and Jennifer Stisa Granick, *The Limits of Location Tracking in an Epidemic*, ACLU (2020) https://www.aclu.org/wp-content/uploads/publications/limits_of_location_tracking_in_an_epidemic.pdf.

[3] *Wi-Fi RTLS, Location Tracking & Positioning*, InPixon, https://www.inpixon.com/technology/standards/wifi (last visited Apr. 11, 2025).

[4] Alex Whitney, "Terms and Conditions, What Do They Mean? Should We Read Them," KGHI (Nov. 19, 2019, 6:30 pm), https://nebraska.tv/news/local/terms-and-conditions-what-do-they-mean-should-we-read-them.

enforcement.[5] This practice allows law enforcement to bypass traditional legal safeguards—such as warrants or subpoenas—gaining access to sensitive personal data without proper oversight or transparency.

In recent years, law enforcement has increasingly used location data by applying for geofence warrants as an investigative tool. Google's Location History feature—also known as "Timeline"—has been the primary source of this data, as it combines multiple technologies, including GPS, Wi-Fi, and cell signals, into a single dataset. This feature is active whenever a user enables Google to store their location data, and it continues to record information indefinitely, providing ongoing default consent unless the user actively turns it off. While location history data can be a valuable investigative tool, it also poses enormous privacy risks if not handled with the utmost care.

[5] *Data Brokers*, ELEC PRIV. INFO. CTR., https://epic.org/issues/consumer-privacy/data-brokers/ (last visited Apr. 11, 2025).

What is a Geofence Warrant?

A geofence warrant, also known as a reverse-location warrant, is a request from law enforcement to an entity possessing location data—typically a technology company—to provide all location history data for devices that were within a defined geographic area during a specific time frame.[6] The duration and geographic scope of geofence warrant requests can, in theory, vary significantly. However, the exact parameters of geofence warrants that have been granted or denied are often difficult to determine. This is because those details are typically disclosed only when a prosecution results, as part of the government's obligation to share evidence with defendants. When a geofence warrant does not lead to criminal charges, its parameters generally remain unknown.

[6] Prathi Chowdri, *Emerging Tech and Law Enforcement: What Are Geofences and How Do They Work?* LEXIPOL (Jan. 4, 2024), https://www.lexipol.com/resources/blog/emerging-tech-and-law-enforcement-what-are-geofences-and-how-do-they-work/.

The most well-known examples of executed geofence warrants are found in the *Chatrie* and *Smith* cases. In *Chatrie*, the geofence warrant covered a search area with a 150-meter radius for a duration of one hour.[7] Assuming the search area was circular, this yields a search area of just under 71,000 square meters, which is the size of roughly 13 football fields, or 3¼ blocks in midtown Manhattan. By contrast, in *Smith*, the warrant authorized an hour-long search within a geofence encompassing approximately 98,192 square meters (equivalent to almost 19 football fields).[8]

[7] United States v. Chatrie, 107 F.4th 319, 324 (4th Cir. 2024), *reh'g en banc granted*, No. 22-4489, 2024 WL 4648102 (4th Cir. Nov. 1, 2024) (hereinafter "Chatrie II").

[8] United States v. Smith, 110 F.4th 817, 827 (5th Cir. 2024).

According to Google, geofence warrants do not seek information about a known suspect or person of interest.[9] Rather, "these requests broadly seek to identify all Google Location History ("LH") users whose LH data suggests that they were in a given area in a given timeframe—even though law enforcement has no particularized basis to suspect that all of those users played a role in, or possess any

[9] Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant (ECF No. 29) at 3, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (hereinafter "Google Amicus Brief").

information relevant to, the crime being investigated."[10]

[10] Id. at 3.

The Current State of the Law

The current process for obtaining a geofence warrant has largely been shaped by Google, given its role as the primary recipient of such orders. In *Chatrie*, the Eastern District of Virginia, citing Google's amicus brief, acknowledged this influence:

> To ensure privacy protections for Google users... Google instituted a policy of objecting to any warrant that failed to include [de-identification] and narrowing measures." Seemingly developed as a result of Google's collaboration with CCIPS [Computer Crime and Intellectual Property Section of the Department of Justice], this deidentification and narrowing "protocol typically...entails a three-step process.[11]

[11] United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022), aff'd, 107 F.4th 319 (4th Cir. 2024) (hereinafter "Chatrie I").

Below, we describe the three-step process employed by Google and followed by law enforcement agencies in directing geofence warrant applications to courts.

The Geofence Three-Step

Step 1 To begin the process, "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."[12] *Chatrie* highlights that "in response to the warrant, Google must 'search ... *all* [LH] data to identify users' whose devices were present within the geofence during the defined timeframe."[13] Google then provides law enforcement with a "production version" of the responsive users' data, which includes:

- an anonymized device number,
- the latitude and longitude coordinates,
- a timestamp of the reported location information,
- the map's display radius, and
- the source of the reported location information (i.e., Wi-Fi, GPS, or a cell tower).

[12] NACDL Fourth Amendment Center, *Geofence Warrant Primer*, Nat'l Ass'n of Crim. Defense Lawyers (Aug. 29, 2023), https://www.nacdl.org/getattachment/816437c7-8943-425c-9b3b-4faf7da24bba/nacdl-geofence-primer.pdf.

[13] *Chatrie I*, 590 F. Supp. 3d at 915.

Step 2 In the second step—which is optional and does not occur for all geofence warrants—law enforcement reviews the production version of the responsive users' data to identify devices of interest.[14] According to Google:

If additional anonymized location information for a specific device is necessary to eliminate false positives or otherwise determine

[14] Google Amicus Brief, *supra* note 9, at 13.

whether that device is actually relevant to the investigation, law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request.[15]

[15] *Id.*

Importantly, Google imposes no geographic limitations on the additional data requested during this step, although it typically requires law enforcement to narrow the number of devices or users identified in Step 1.[16] Step 2 is optional and is rarely implemented in practice—presumably because there are no legal restrictions on law enforcement's ability to seek de-anonymization of the data obtained in Step 1 during the third step of the process, as described below.

[16] *Chatrie I,* 590 F. Supp. 3d at 916.

Step 3 The final step in the geofence process involves de-anonymization. At this stage, the government can "compel Google . . . to provide account-identifying information for the users. . . relevant to the investigation." [17] This information typically includes the name and email address associated with each account. [18] Google appears to prefer that law enforcement request de-anonymized data for fewer users than those identified in Step 2.[19] However, the fact that a private company effectively determines how much data to de-anonymize in response to a government request is concerning—especially given the potential for coercive tactics by the government.

[17] *Id.*

[18] *Id.*

[19] *Id.*

Academic Perspectives on Geofence Warrants

Courts and legal scholars have conflicting views regarding the constitutionality of geofence searches. For example, the Fifth Circuit in *United States v. Smith*[20] held that geofence warrants are outright unconstitutional, while the Fourth Circuit in *United States v. Chatrie*[21] held that limited geofence searches are not "searches" as that term is defined in the Fourth Amendment.[22] Legal scholars are similarly divided on the constitutionality of geofence searches specifically, and on law enforcement warrants that seek access to privately held data more broadly.[22] Some argue that geofence searches violate the Fourth Amendment due to data privacy implications,[23] the lack of judicial oversight associated with current geofence searches,[24] and unchecked officer discretion.[25] However, many others argue that geofence searches could be constitutional with proper safeguards,[26] though there is much disagreement as to what those safeguards might be.

[20] *Smith*, 110 F.4th at 840.

[21] *Chatrie I*, 590 F. Supp. 3d at 941 (4th Cir. 2022).

[22] *See, e.g.*, Ronald J Rychlak, *Geofence Warrants: The New Boundaries*, 93 Miss. L. J. 957; Emily Brodner, *Navigating the Terrain of Geofence Warrants*, 7 Ariz. L. J. Emerging Tech. 2 (2024);; Denise Cespedes, *Uncharted Boundaries: Exploring Geofence Warrants as an Investigative Tool in Abortion-Related Criminal Investigations Post-Roe*, 34 U. Fla. J. L. & Pub. Pol'y 41 (2023).

[23] Haley Amster & Brett Diehl, *Against Geofences*, 74 Stan. L. Rev. 385, 437 (2022).

[24] *Geofence Warrants and the Fourth Amendment*, 134 Harv. L. Rev. 2508, 2514 (2021).

[25] Josh A Roth, *Drawing Lines: Geofence Warrants and the Third-Party Doctrine*, 4 Int'l Cybersecurity L. Rev. 1, 8 (2023).

[26] *See generally* Jane Bambauer, *Filtered Dragnets and the Anti-Authoritarian Fourth Amendment*, 97 S. Cal. L. Rev. 571, 635 (2023); Reed Sawyers, *For Geofences: An Originalist Approach to the Fourth Amendment*, 29 Geo. Mason L. Rev. 788, 825 (2022); Magistrate Judge Beth W. Jantz, *Simulating More Particularity: Ideas for Approaching Search Warrants for Geofences, Tower Dumps, and Cell-Site Simulators*, 16 Fed. Cts. L. Rev. 9, 19-30 (2024).

The Changing Location Data Environment

On December 12, 2023, Google officially announced that Location History data would be stored locally on users' devices within the following year, rather than in "SensorVault" service.[27] Furthermore, for users who choose to back up their data to the cloud, Google stated it would "automatically encrypt your backed-up data so no one can read it, including Google." Finally, Google announced that the default auto-delete period for location data would be reduced from 18 months to 3 months. [28]

Recent media reports indicate that Google has now set June 9, 2025, as the final date for the transition of its "Timeline" location history feature from cloud-based to on-device storage. Some Google customers have begun receiving notifications concerning the termination of the service and have been advised that their data will be deleted unless they save it to their device before June 9, 2025.[29]

While Google may no longer be able to provide law enforcement with Location History (LH) data going forward, law enforcement will likely turn to alternative sources, such as app developers, mobile service providers, and data brokers. As previously noted, Google has been the primary recipient of geofence data requests due to its ability to aggregate location information from a variety of technologies. However, there is little to prevent law enforcement from obtaining similar data from other individual or combined sources to construct comparable location history datasets.

In today's app-driven environment, a person's location data may

[27] 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/.

[28] Donna Lee Elm, *Are Geofence Warrants Headed for Extinction?*, Crim. Just. (Aug. 8, 2024), https://www.americanbar.org/groups/criminal_justice/resources/magazine/2024-summer/geofence-warrants-headed-extinction/.

[29] Nathan Drescher, *Google puts a (new) date on Maps Timeline's shutdown*, YahooTech (Dec. 11, 2024, 4:09 PM) https://www.yahoo.com/tech/google-puts-date-maps-timelines-230941507.html.

be held by numerous entities, including internet service providers, mobile carriers, and various apps installed on their devices. Such data is often aggregated by data brokers, and there are no constraints on law enforcement directing geofence warrants at data brokers—or simply purchasing location history data sets from these entities. An investigative report by a consortium of media outlets last year revealed how easily location data could be purchased from data brokers—data that precisely tracked the movements of U.S. military personnel stationed in Germany, from their barracks to brothels located just off-base.[30] Legislation addressing the broader issues posed by the data broker industry is beyond the scope of this document. However, the continued availability of location data on the open market—even after Google sunsets its Location History features—underscores the need for laws regulating how law enforcement uses geofences as an investigative technique.

[30] Dhurv Mehothra & Dell Cameron, *Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany*, WIRED (Nov. 19, 2024, 11:00 am), https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/.

The Need for Legislative Action on Geofence Warrants

Legislatures have a vital role in balancing the investigative value of geofence searches against the serious threats they pose to user privacy. This can be achieved by enacting legislation that defines when and how law enforcement may use geofence searches, along with robust safeguards to protect the privacy of individuals whose information is captured by such warrants.

Legislatures cannot simply leave these questions to the courts. Courts tend to focus on threshold questions of constitutionality, rather than articulating the detailed rules necessary to govern complex technologies and investigative processes. Legislation based on the policy proposed below can therefore:

1. **Establish clear guidelines for law enforcement personnel.** The policy sets clear criteria for when a geofence warrant may be used. It also outlines the factors that must be considered when defining a geofence, ensuring that the geographic and temporal scope is not drawn too broadly.

2. **Ensure the policy is technology neutral.** The policy is designed to be adaptable and broadly applicable. It provides guidelines that apply to any technology or company that collects location data, regardless of the tools or systems they use.

3. **Balance privacy implications with investigative utility.** The policy helps strike a balance between the need for law enforcement to use specialized investigative techniques in serious cases—particularly when conventional methods fall short—and the highly invasive nature of geofence warrants. This is especially important for protecting the privacy of individuals whose location data is disclosed incidentally, due to the broad and indiscriminate nature of geofence data collection.

Policy Considerations

This policy prioritizes the following considerations:

The Fourth Amendment. The Fourth Amendment safeguards against unreasonable searches and seizures.[31] Geofence searches and other forms of electronic surveillance have the potential to capture uninvolved parties' data, making it difficult to reconcile with Fourth Amendment protections. However, this policy applies the same level of caution to geofence searches as other potentially highly intrusive investigative methods, such as wiretaps,[32] to preserve constitutional protections and the technology's utility.

[31] U.S. CONST. amend. IV.

[32] 18 U.S.C. § 2518 (requirements for law enforcement to obtain a warrant for wiretaps and other forms of electronic surveillance).

Privacy Protections. Geofence warrants, like many other surveillance techniques, burden the privacy rights of uninvolved individuals. Location data can reveal sensitive information about an individual's movements, associations, and activities. This policy seeks to minimize the privacy burdens that geofence warrants impose on individuals—including both potential suspects as well as innocent individuals who just happen to be in the same place at the same time a crime was committed.

Exhaustion and Serious Crime Requirements. As geofences can potentially collect any individual's data within a defined area, this policy restricts the use of geofence warrants to serious crimes when conventional investigative methods have been exhausted. These limitations ensure that the technology is not used as a first-line, routine, investigative tool.

Judicial Oversight. Geofence searches constitute a search under the Fourth Amendment and therefore require a warrant. These searches can generate vast amounts of data, potentially revealing highly sensitive information about anyone located within the geofence boundaries. Subpoenas and other less stringent legal mechanisms do not offer the same level of privacy protection or judicial oversight as a warrant. This policy proposes heightened warrant requirements that ensure a neutral judge is involved throughout the entire process. Such oversight helps ensure that geofence searches are used only as a last resort and that a judge carefully evaluates whether the potential privacy intrusions are justified by the investigative need.

A Model State Policy to Govern Geofence Warrants

This policy recommends limiting geofence searches to investigations of serious crimes, and only after other methods have proven unsuccessful or are unlikely to advance the investigation. Additionally, it introduces a "Step 0," requiring law enforcement to subpoena a provider to obtain the number of devices that would fall within the proposed geofence. These additional safeguards aim to limit officer discretion and enhance judicial oversight, allowing all parties to better assess the potential privacy risks involved.

Defining Geofence Warrants

For purposes of this policy, a "geofence warrant" refers to any demand, request, or other legal process issued by law enforcement to a third party compelling the production of records or data concerning the geographic location of one or more devices, where such records or data meet the following criteria:

1. **Precise Location:** The data originates from any technology capable of identifying the location of an individual within a radius of 1850 feet. [33] This includes, but is not limited to, geographic coordinates (e.g., latitude and longitude) derived from technologies such as GPS, cell site location information (CSLI), Wi-Fi positioning, Bluetooth tracking, or similar methods; and

2. **Real-Time or Retrospective Collection:** The location data is either collected in real time or stored by a third party as part of its routine data collection practices; and

3. **Source: Devices or Objects:** The data originates from electronic devices such as mobile phones, smartwatches, or other connected technologies, or from physical tracking tools such as location tags or similar mechanisms.

Exclusions: This definition does not include records or data derived from indirect indicators of location, such as:

[33] This number is based on the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"), Cal. Civ Code §§ 1798.140 (ae), the degree of accuracy and precision for Geolocation Data is a radius of 1,850 feet or less. Whereas, under other state privacy laws, the radius is 1,750 feet or less.

1. Transactional records, including—but not limited to—credit card purchases, bank transactions, or other financial activities;

2. Publicly available information, such as social media posts or public records; or

3. Data sources in which location is inferred solely from contextual or non-geographic information, such as healthcare records, employee databases, or customer interaction logs, where location may be deduced from patterns of communication or service usage.

Conditions Governing the Availability of Geofence Warrants

The Serious Predicate Offense Requirement

It is critical to limit geofence warrants to serious crimes that may justify the significant privacy intrusions they entail—a limitation that also applies to other highly invasive surveillance techniques, such as wiretaps. Recognizing that definitions of criminal severity vary by state, geofence warrants should be permitted only for offenses classified as the most serious under state law, typically involving violence or severe harm.

The existence of a predicate offense alone does not justify the issuance of a geofence warrant. However, the seriousness of the underlying crime is a key factor in determining whether such a warrant may be appropriate. While more serious crimes may warrant the use of a geofence, less serious offenses are unlikely to meet that threshold. Even in cases involving predicate offenses, law enforcement must still address all additional considerations—such as the geofence's timeframe, its geographic scope, the population density of the area to be searched, and other tailoring factors—to ensure the search is narrowly constrained so as to mitigate privacy risks.

To ensure consistent and appropriate application, states may choose to define predicate offenses that justify a geofence search using the following:

- **The State's Most Serious Felonies.** Geofences should be reserved for the state's most serious felonies, such as Class A or Class 1 felonies, which usually involve imminent harm, violence, or destruction.[34]

- **The State's Wiretap Statute.** If the state's wiretap statute is restricted to Class A and/or serious violent felonies, states have the option to use the existing wiretap laws to define predicate offenses.

[34] In states without felony classifications, legislators must decide which serious crimes warrant geofence searches. These searches should be limited to the most severe crimes, such as those punishable by death or life imprisonment.

Probable Cause

The Fourth Amendment's requirement of probable cause[35] is an important narrowing factor on the issuance of geofence warrants that prevents their overuse. As applied to geofence warrants, the probable cause requirement would be met by law enforcement establishing that the temporal duration and spatial extent of the information sought from a provider is narrowly tailored to obtain evidence of the predicate offense. Correspondingly, affidavits supporting geofence warrant applications must explain why the time and extent of the information being sought is necessary, and why no shorter duration or narrower extent would suffice.

To establish probable cause for a geofence warrant, the affidavit must include:

Probable Cause to the Geofence's Temporal Duration. Law enforcement must articulate specific facts to establish probable cause for the geofence's entire temporal duration, rather than a shorter duration. This requirement restricts law enforcement from requesting a timeframe that will not yield evidence of the commission of the predicate offense.

Probable Cause for the Geofence's Spatial Extent. Law enforcement must articulate specific facts that meet the probable cause standard to establish that the geofence's full spatial extent, and not a smaller spatial area, will provide evidence of the commission of the predicate offense.

[35] U.S. CONST. amend. IV.

Exhaustion Requirements

This policy seeks to ensure that geofence warrants are not issued prematurely, routinely, or without careful consideration. They should be used only when other investigative methods have been exhausted, in order to balance the significant privacy interests at stake with law enforcement's investigative needs. The exhaustion requirement is designed to prevent the use of highly intrusive electronic surveillance techniques in situations where less intrusive methods would be adequate.[36]

Before seeking a geofence warrant, law enforcement must first attempt to exhaust conventional investigative approaches, such as in-person witness interviews or a targeted review of the location data of an identified suspect. These less invasive methods can often yield similar results without exposing large numbers of innocent bystanders to surveillance. Alternatively, if traditional techniques are unlikely to advance the investigation—for example, in remote areas lacking surveillance infrastructure or eyewitnesses—law enforcement must explain why those methods are insufficient and demonstrate

[36] *Cf.* 18 U.S.C. § 2518(3)(c) (requiring law enforcement to exhaust traditional investigative techniques before obtaining a warrant for wiretaps and other forms of electronic surveillance) ("normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous").

why a geofence search is highly likely to produce meaningful investigative leads.

Judicial Oversight and Accountability

Given the potential for overreach and the significant privacy concerns associated with geofence warrants, judicial oversight is critical. Judges reviewing geofence warrant applications must ensure that the requests meet specific legal and factual standards. Applications should include a clear rationale for why a geofence warrant is necessary and why less intrusive alternatives would not suffice. Supporting affidavits must contain specific, detailed statements; generalized or conclusory assertions are inadequate and should not be accepted.

When requesting a geofence warrant, law enforcements affidavits must provide a detailed and complete statement that meets the following conditions:

1. A full and complete statement of the facts and the predicate offense;
2. Probable cause establishing the timeframe and geographic location of the predicate offense;
3. Specific reasons why the geofence warrant is likely to further the investigation of the crime;
4. An estimate of the amount of data the geofence will gather (*i.e., the data gathered in Step 0*); and
5. Alternative investigative procedures:
   (a) That have been tried and failed; or
   (b) That are reasonably unlikely to succeed if employed; or
   (c) Are too dangerous to employ.

While reviewing the affidavit, an issuing judge must consider the following factors:

- The specific crime in question and whether it is a predicate offense;
- The specificity and completeness of the law enforcement's statement;
- Whether probable cause has been established for the location and timeframe of the geofence search;
- Whether law enforcement has reasonably exhausted other investigative techniques; and

- Whether the impacts on the privacy interests of uninvolved parties are reasonable under the circumstances (amount of data from Step 0, density, timeframe).

Illustrative Examples

Predicate Offense:

- **Likely Unacceptable Crime:** A petty theft would not justify a geofence warrant because it is not a serious crime that involves harm, violence, or destruction.
- **Likely Acceptable Crime:** A string of arsons is likely to justify a geofence warrant because arson is a serious crime that could involve harm, violence, and/or destruction.

Probable Cause:

- **Probable Cause to the Geofence's Timeframe.** A one hour timeframe is likely to capture the device of someone who is suspected of committing two arsons within an hour of each other. A shorter timeframe would not cover both arsons.
- **Probable Cause to the Geofence's Geographic Coordinates.** A narrow perimeter drawn around each arson site is sufficient to gather data to determine if the same device was present in and around both crime scenes at the time the arsons were set. However, a geofence that covers the space between the two arson sites is overbroad, as it is not necessary under the circumstances to identify a serial arsonist.

Exhaustion of Alternative Investigative Procedures:

- Alternative investigative techniques (e.g., canvassing local residents, forensic investigations) have not yielded any useful evidence to help identify a suspect.
- The nature of the public safety risk posed by the crime justifies the use of a highly invasive investigative technique, as conventional techniques are unlikely to yield evidence useful to identifying a suspect.

Other Factors Establishing the Necessity of the Geofence Warrant:

- The crime occurred in an isolated, rural area where there are no eyewitnesses, no security cameras, and no useful forensic evidence to identify the suspect.
- Forensic evidence was destroyed by the nature of the crime committed (e.g., an arson).

Tailoring Factors

When designing a geofence, several factors can help ensure that the scope of the request is appropriately limited and not overly invasive. While no single factor is dispositive, these considerations can guide judges and law enforcement in evaluating the volume and sensitivity of the information being sought. Greater judicial scrutiny is warranted when a geofence risks deanonymizing sensitive data. The following factors are intended to help balance the seriousness of the crime under investigation with the breadth of information requested through the geofence.

1. **The geographic area requested.** A large geographic area weighs against a geofence warrant being granted while a confined area makes a geofence more likely to be granted. The government should be able to articulate why the requested geographic area is likely to return the evidence being sought, but a more narrowly tailored geographic area would not.

   All other factors being equal, a geofence warrant for a fatal shooting that occurred in a parking lot is more likely to be granted if confined to the parking lot in which the crime occurred, as opposed to the entire block within which the parking lot is located.

2. **The timeframe being requested.** Similarly, an application seeking information for a prolonged period weighs against the granting of a geofence warrant, while a constrained time weighs in favor. The government should be able to articulate why the requested timeframe is necessary to return the evidence being sought, whereas a narrower timeframe will not do.

   All other factors being equal, a judge should be more likely to grant a geofence warrant for an armed robbery of a jewelry store if it is constrained to the time the robbers were in the store, as opposed to an hour before or after the robbery.

3. **The population density of the area.** A geofence warrant should be less likely granted in a densely populated area.

   All other factors being equal, a geofence warrant for a crime committed on the plains of eastern Colorado is more likely to be granted than that for the same crime committed in Times Square on New Year's Eve.

4. **Typical building use in the area.** If the geofence includes particularly sensitive locations—such as residences, places of worship, or health clinics—that should weigh against granting the request. The government should be required to identify and describe the types of buildings located within the proposed geofence in its application. A failure to provide specific information or clear statements

regarding the presence of sensitive locations should also weigh against approval of the geofence warrant.

> All other factors being equal, law enforcement would be more likely to have their geofence warrant request approved for a warehouse than for a strip mall that contains a medical clinic, a sex shop, and a storefront church.

None of these factors are independently dispositive. They are interconnected, and each situation should be evaluated on a case-by-case basis, taking all relevant factors into account. To reiterate, the goal of this proposal is to strike a balance between the significant privacy concerns raised by geofence warrants and their potential effectiveness as a law enforcement tool—ensuring that justice can be served without compromising fundamental rights.

An Enhanced Multi-Step Geofence Warrant Process

Step 0: Particularization to Location

This step is a key innovation introduced by this policy to improve judicial decision-making. Known as "Step 0," it requires law enforcement to demonstrate that they have defined the smallest feasible area necessary to obtain information required for their investigation. In our view, this step can serve as a meaningful way for law enforcement to tailor geofence warrant requests to reduce the privacy impact of these searches on innocent individuals who happen to be in the vicinity of a serious crime being committed.

Before compelling an entity—such as a phone carrier, internet service provider, or other platform that retains location history data—to produce location information, law enforcement should first issue a subpoena requesting information about the number of devices that are located with a proposed geofence for a given time. Law enforcement should attempt to draw the geofence as narrowly as possible, minimizing the number of devices implicated. In doing so, they must account for the same privacy concerns that would be relevant to a full geofence warrant application, including the presence of sensitive locations, population density, proximity to major roadways, and similar contextual factors.

The device count obtained from the subpoena would help law enforcement assess both the effectiveness and the proportionality of a potential geofence warrant. Furthermore, if multiple subpoenas are made and the number of affected devices is successfully narrowed, this information can serve as additional support for a subsequent warrant request.

It is also important to distinguish between one large geofence and several smaller, targeted geofences. A single broad geofence risks sweeping in data from many individuals unnecessarily, whereas multiple, narrowly drawn geofences may better reflect available information about a suspect's movements and allow law enforcement to cross-reference suspect devices. In such cases, law enforcement could request data showing how many devices appear in one or more proposed geofence areas. For example, if investigators know that a suspect fled in a certain direction or traveled to a specific destination, a court may be more inclined to authorize two narrowly tailored geofences for comparison. This approach reduces the risk of excessive privacy intrusions while increasing the likelihood of correctly identifying the suspect.

Step 1: Warrant Application for Anonymized Location Information:

Ideally, after receiving the number of devices from Step 0, law enforcement would proceed to request a search warrant to obtain device geolocation data. Geofence warrant applications must include the number of devices identified in the initial subpoena (if applicable), explain why the proposed geographic boundaries and timeframe are narrowly tailored, and satisfy the probable cause and particularity requirements.

Judges reviewing the warrant application should consider the relevant tailoring factors, the use and effectiveness of traditional investigative tools, the overall benefit to law enforcement, and any other contextual factors to ensure the request is sufficiently narrowly tailored. Importantly, law enforcement should take special care to avoid sensitive locations, such as residences, places of worship, hospitals, or health clinics, within the geofence. If the judge determines that the geofence could be drawn more narrowly, they should direct law enforcement to revise it accordingly.

Step 2: Tailoring and Additional Information

For a narrow subset of devices identified in Step 1, law enforcement may request to expand the temporal scope of the geofence, subject to reasonable time limitations, through a court order. This step involves similar considerations as the initial warrant but applies a different legal standard.

Rather than applying the probable cause standard required for warrants or the minimal threshold of mere suspicion used for subpoenas, this policy proposes using the intermediate standard set forth in 18 U.S.C. § 2703(d). Under this standard, law enforcement must demonstrate "reasonable grounds to believe" that the informa-

tion sought is both "relevant and material" to the ongoing investigation. This creates a more tailored and proportionate approach to Step 2 that appropriately reflects the privacy implications of expanding the geofence.

Under Google's current three-step process, Step 2 lacks mandatory judicial oversight, and law enforcement is not required to provide additional justification or narrow their suspicions before obtaining further information. The proposed intermediate standard remedies that deficiency by introducing judicial oversight while avoiding undue burdens on law enforcement.

Requests to courts at the second step may only be made when law enforcement needs additional information—such as an expanded timeframe—about data obtained through the initial search warrant. The request must explain why the expanded data is necessary and how the pool of devices has been substantially narrowed. This phase may be repeated as needed, provided the requirements are met each time.

While Step 2 is optional, it is strongly encouraged. It offers clear benefits for both law enforcement and individuals whose data may have been swept into the initial geofence. For individuals, this step creates an additional opportunity to be excluded from further investigation before their data is deanonymized. For law enforcement, Step 2 serves two important functions: (1) it permits access to additional data and investigative avenues, and (2) it may help establish probable cause for the next phase—Step 3—by providing a stronger basis for a subsequent search warrant.

Step 3: Deanonymization

Ideally, by this stage in the process, law enforcement has already eliminated many of the devices initially identified in Step 0. Those devices would have been further scrutinized and narrowed during Step 1, and possibly even more so in Step 2. At this point, only a small number of suspect devices should remain—devices that law enforcement may seek to de-anonymize. However, de-anonymization carries the greatest privacy implications of the entire process. Accordingly, this step requires a new search warrant supported by probable cause.

Under current law, no judicial involvement is required beyond the initial warrant. In contrast, this policy keeps the courts actively involved as an essential check on law enforcement's power throughout the entire geofence search process.

To de-anonymize devices identified in previous steps, law enforcement must obtain a new search warrant. Applications for such war-

rants must be supported by probable cause that the device in question belongs to the individual who committed the alleged crime—not merely that the device was present within the geofence. The standard also includes an exhaustion requirement: law enforcement must demonstrate that less invasive methods have been pursued and have not yielded useful results. The warrant application must meet the particularity requirement and substantially limit the number of devices to be de-anonymized relative to those identified in Steps 1 and 2.

Law enforcement may not use de-anonymized information to investigate or prosecute individuals for offenses unrelated to the crime under investigation. Nor should the information be used for any purpose other than solving the specific crime that justified the geofence warrant in the first place.

Judges reviewing a Step 3 request must consider how many devices are proposed for de-anonymization and revisit the same factors applied in Step 2—balancing investigative necessity against privacy risks.

Post Acquisition Standards

There are several post-acquisition issues and standards that apply more broadly and fall outside the scope of this brief. These include data retention, access restrictions, search protocols, and minimization requirements. However, one standard we strongly endorse is a notification requirement.

Once law enforcement advances to a subsequent stage of the geofence process, any data—anonymized or not—that is no longer necessary to further the investigation must be promptly destroyed. Specifically, any device and corresponding location information that cannot support a showing of probable cause to believe it belongs to the perpetrator must be deleted.

Notification

Providers that collect location data are encouraged to notify users when their data has been collected and subjected to a geofence search, once it is lawful and no longer risks compromising the investigation. However, because most data provided to law enforcement is anonymized, this policy also recommends adopting an annual reporting requirement similar to the one mandated by the Wiretap Act.[37] That Act requires a yearly report detailing all applications for wire, oral, or electronic interceptions made by state and federal authorities.[38]

[37] Title III of The Omnibus Crime Control and Safe Streets Act (Wiretap Act) of 1968, 18 U.S.C. §§ 2510-2523.

[38] 18 U.S.C. § 2519 (requiring annual reports from judges and law enforcement detailing warrant applications, approvals, interceptions, arrests, trials, and convictions be sent to Congress).

To promote transparency, geofence warrants should be subject to a similar reporting regime. This system would ensure that key details—such as the frequency, purpose, and outcomes of geofence searches—are documented and made available for oversight. Regular reporting would create a public and judicial record to help prevent misuse and foster accountability.

A yearly report should include:

1. A general description of the geofence searches conducted in the state, including:
   (a) The approximate nature and frequency of successful geofence warrants that resulted in arrests;
   (b) The approximate nature and frequency of unsuccessful geofence warrants that did not result in arrests;
   (c) The approximate number of uninvolved persons whose data was collected in each successful and unsuccessful geofence search; and
   (d) The approximate nature, amount, and cost of the human and other resources used in conducting the searches.
2. The number of arrests resulting from successful geofence warrants, and the nature of the offenses for which arrests were made.
3. The number of trials resulting from such geofence warrants.
4. The number of convictions resulting from geofence warrants.

Retention

Law enforcement must limit the use of geofence data to the specific crime identified in the original warrant application. The scope of the search must be narrowly tailored to the relevant investigation, ensuring that unrelated or extraneous data is neither accessed nor used. Any data obtained through a geofence search that does not pertain to the specified crime must be excluded from the investigation. Strict adherence to this principle safeguards privacy and ensures that law enforcement actions remain lawful, focused, and appropriately restrained.

Broader Policy Proposals

Regardless of the specific rules governing the use of geofence warrants, lawmakers must take special care to address the privacy concerns associated with the technologies used to create and store location data in the first place. Law enforcement can also circumvent the

warrant process through other means—most notably, by purchasing location history information from data brokers.[39] Limiting geofence warrants is necessary but insufficient on its own. Complementary policies focused on data retention, minimization, and restrictions on third-party data sales are essential to strengthening privacy rights in the digital age.

[39] Ángel Díaz, When Police Surveillance Meets the 'Internet of Things', BRENNAN CTR. FOR JUST. (Dec. 16, 2020) https://www.brennancenter.org/our-work/research-reports/when-police-surveillance-meets-internet-things ("[C]onnected devices provide new ways to obscure those practices by obtaining data from cooperative landlords or employers instead of having to comply with transparency and accountability controls beginning to take root around the country."); *After House Passes Fourth Amendment Is Not For Sale Act, ACLU Urges Senate to Stop Government from Spying on Americans Without a Warrant*, ACLU (Apr.17, 2024 6:00 PM) ("[F]or years now, federal agencies, including the Internal Revenue Service and the Department of Defense, have been buying their way around this requirement by purchasing Americans' sensitive information from data brokers.").

Conclusion

The proposal outlined above offers several key benefits that balance the vital importance of safeguarding civil liberties with the legitimate investigative needs of law enforcement in using geofence warrants in exceptional circumstances.

1. **Establishes threshold requirements for appropriate application.** Not all crimes warrant the use of a geofence. By specifying threshold conditions under which a geofence warrant may be issued, this policy ensures that such warrants are granted only in cases where they are truly necessary to investigate serious crimes.

2. **Specifies tailoring factors to ensure narrowly drawn geofence warrants.** In circumstances where a geofence warrant is necessary, tailoring its geographic and temporal scope is critical to protecting individual privacy. This policy identifies key factors law enforcement should use to draw appropriately limited geofences, and provides a framework for judges to evaluate whether a warrant is sufficiently narrow to meet constitutional and policy standards.

3. **Maintains requirements on law enforcement to demonstrate need at each stage.** This policy applies escalating standards of proof at different stages of the process. At earlier stages, a subpoena may suffice to help law enforcement assess the scope of the data requested. As the process advances and privacy implications increase, higher standards—such as probable cause—are required. This tiered approach ensures that geofence warrants remain available as an investigative tool, but only when law enforcement can demonstrate their necessity under heightened scrutiny.

4. **Encourages supplemental procedures, including notification requirements.** User privacy interests are implicated at every step of the geofence process—from the Step 0 subpoena requirement to the deletion of irrelevant data at the end of the process. Correspondingly, we have proposed user notification requirements as well as public transparency requirements to ensure that judges,

legislators, and ordinary citizens can surveil the use of this powerful investigative technique.

This model policy proposal addresses a significant gap in Fourth Amendment jurisprudence. It recognizes both the substantial privacy implications of geofence warrants and their practical value in aiding investigations that might otherwise remain unresolved. The proposal builds on the current legal framework, draws from analogous tools and statutes, and incorporates the recommendations of leading scholars in the field. In short, it establishes an iterative system in which judicial oversight is applied at each stage of the investigative process, using graduated legal standards that reflect the increasing privacy concerns as the investigation progresses.