Connecticut Debate Association
March 7, 2026
Stamford High School and Farmington High School

THW prohibit geofence warrants.

Contents

Supreme Court agrees to decide if police can seek sweeping cellphone location data in investigations

CNN, by John Fritze 01/16/2026

The Supreme Court agreed Friday to review whether police warrants that allow access to large amounts of cellphone location data to identify people near a crime scene are constitutional.

The practice of issuing geofence warrants has divided lower courts, some of which have ruled that it constitutes the kind of sweeping warrants that are prohibited under the 4th Amendment.

The high court has been considering at least two appeals on the issue in recent weeks. One came from a man convicted of robbing a bank in Virginia in 2019 who was identified after police collected cellphone location data from Google.

Police were able to identify cellphones that pinged location data to apps near crimes. They were then able to identify the phone's owner. But in the process, the appeals allege, the police obtained anonymized location data from millions of other people who were not involved in crimes.

Eight years ago, a divided Supreme Court ruled that law enforcement generally needed to establish probable cause before accessing cellphone tower data to identify suspects. In that case, Chief Justice John Roberts was in the majority with the then four-justice liberal wing. Three current justices – conservatives Clarence Thomas, Samuel Alito and Neil Gorsuch – were in dissent.

In the Virginia case, police say Okello Chatrie passed a note urging a bank teller to "hand over all the cash" and that he needed "at least 100k and nobody will get hurt and your family will be set free." Initially, police were unable to identify a suspect, but officers noticed on security cameras that the suspect was using his phone prior to the robbery. Law enforcement served a geofence warrant on Google seeking location data for every device near the bank within an hour of the robbery.

Chatrie was later convicted of armed robbery and sentenced to more than 11 years in prison.

"When magistrate judges receive requests for geofence warrants, they need to know what rules apply," his attorneys told the Supreme Court. "The same is true for tech companies that wish to cooperate with law enforcement while also protecting their users' privacy and complying with the Constitution."

The federal government has argued that the warrants do not constitute a search for 4th Amendment purposes and it notes that users must opt in to location services on their phones, which they might do in order to access real-time traffic information, for instance.

Google, which received most of the warrants, changed its policy last year to shift how the data is stored so that it is far harder to comply with the warrants. Because of that, the federal government told the Supreme Court, the case is effectively moot.
"Google's policy change," the government said, "significantly diminishes the frequency with which geofence-warrant issues will arise in future prosecutions."

Supreme Court agrees to hear a Fourth Amendment case regarding geofence warrants

Brookings Institute, by John Villasenor January 27, 2026

The Fourth Amendment protects people from "unreasonable searches and seizures" by the government. Interpreting that protection in light of evolving technology often leads to novel constitutional questions. On Jan. 16, the Supreme Court agreed to consider one such question, granting a petition to hear a case involving the constitutionality of geofence warrants. Argument in the case, Chatrie v. U.S., will likely be scheduled for the spring, with a decision expected by early summer.

What are geofence warrants?

Geofence warrants require a company—often Google—to turn over information regarding the devices that it tracked within a targeted area over a time period of interest. As the supplier of the Android operating system and of apps like Google Maps that run on both iPhones and Android devices, Google has access to an enormous amount of location data. Until at least late 2023, Google stored this information in a centralized repository called Sensorvault, though in December 2023, the company announced it would start migrating the data to people's personal devices. Whether and to what extent that migration has occurred is difficult to determine.

In response to the rapid growth in the use of geofence warrants by law enforcement starting in the late 2010s, Google developed a multistep process for responding to them. Initially, law enforcement provides Google, via the warrant, geofence information specifying a window in space and time associated with a crime. Google responds by providing the location history for devices it tracked within the geofence. In this initial response, the devices are "de-identified," so that while law enforcement receives detailed location information regarding the tracked devices, each device is identified only by a number that (in theory, but not necessarily in practice) does not reveal the identity of the device owner.

After analyzing the tracking data, law enforcement can narrow the focus to particular devices of interest and can order Google to provide location data for those devices outside the time and location of the geofence. As a final step, law enforcement can order Google to de-identify devices by providing the associated names or email addresses.

The Chatrie case

Chatrie v. U.S. arose from a credit union robbery in Virginia in 2019. Using a geofence warrant, law enforcement identified Okello Chatrie as a suspect and charged him with several federal crimes. In the subsequent proceeding in a Virginia federal court, Chatrie sought to suppress the evidence from the geofence warrant, arguing that it violated the Fourth Amendment. The district court concluded that "because the Government Lacked Particularized Probable Cause as to Every Google User in the Geofence," the warrant was indeed unconstitutional. However, the court declined to suppress the evidence, citing the "good faith" exception.

Normally, under the "exclusionary rule," evidence obtained through a search that violates the Fourth Amendment cannot be used at trial. But there is an exception recognized by the Supreme Court in 1984: If law enforcement conducts an unconstitutional search on the good faith belief that the search is not unconstitutional, a court can permit the evidence to be used at trial despite the violation.

After failing to obtain suppression of the evidence at the district court, Chatrie appealed to the Fourth Circuit, which handles most appeals from federal district courts in Virginia, West Virginia, and the Carolinas. In July 2024, a three-judge panel issued a 2-1 decision agreeing with the district court that the evidence should not be suppressed but citing a different reason: "Chatrie did not have a reasonable expectation of privacy in two hours' worth of Location History data voluntarily exposed to Google. So the government did not conduct a search when it obtained this information from Google." Under this reasoning, since there was no "search," there was no Fourth Amendment violation.

Chatrie then asked for an "en banc" re-hearing before the full Fourth Circuit, which in April 2025 issued an unsigned, one-sentence opinion joined by 14 of the 15 judges and affirming the district court's decision to deny suppression of the geofence evidence. That decision was accompanied by eight concurring opinions and a single dissent that collectively spanned over 100 pages. In July 2025, Chatrie submitted the petition that the Supreme Court has now granted.

A fractured landscape

As if the collection of district and circuit court opinions in Chatrie weren't complicated enough, courts in other jurisdictions have adopted different approaches to the question of geofence warrant constitutionality. In 2024, the Fifth Circuit, which covers Texas, Louisiana, and Mississippi, concluded in U.S. v. Smith that geofence warrants "are modern-day general warrants and are unconstitutional under the Fourth Amendment." The Fifth Circuit nonetheless invoked the good faith exception, allowing the evidence from the geofence warrant at issue to be used. Additionally, in April 2025, the Texas Court of Criminal Appeals—the state's highest criminal court—ruled in Wells v. State that "use of the geofence warrant in this case to obtain location history data did not violate the Fourth Amendment." This creates an odd situation where geofence warrants are now presumptively constitutional in Texas state courts, but not in Texas federal courts.

Opt-in location data and an expectation of privacy

The arguments before the Supreme Court will focus on the question of whether people have a reasonable expectation of privacy in the location history data collected by Google—and by implication by other app providers as well.

Under the third-party doctrine, which was articulated half a century ago in a very different technological environment, a person does not have a reasonable expectation of privacy in information voluntarily conveyed to a third party. The government can thus obtain that information directly from the third party without running afoul of the Fourth Amendment.

But the contemporary scope of the third-party doctrine is unclear. In 2018, in Carpenter v. U.S., the Supreme Court ruled that information maintained by mobile network providers regarding which cell towers their subscribers' phones were connected to does not fall under the third-party doctrine. If the government wants cell site information, it needs a warrant. Carpenter left open the question of Fourth Amendment protections for other forms of location data collected by mobile phones and other personal electronic devices.

While the Supreme Court argument is a few months away, key aspects of the parties' positions are presented in the petition and the government's response. Chatrie underscores that Google's location data, because they are based on signals from GPS satellites and nearby Wi-Fi hotspots, are far more precise than the cell site data at issue in Carpenter. Chatrie argues that a warrant should certainly be required to obtain location data that are substantially more accurate than that considered in Carpenter. Chatrie also explains that while prosecutors in Carpenter obtained location data for a handful of mobile phones, a geofence warrant is even more invasive as it seeks location data for all devices in the geofence.

The government argues that Carpenter is inapplicable to geofence warrants. The government points out that unlike cell site data, which are collected automatically when a phone connects to a cell network, Google's location data are opt-in. The government invokes the third-party doctrine, arguing that Chatrie "voluntarily shared his cellphone location with Google by opting in to the Location History service, thus relinquishing any privacy right in that information." The government also underscores that the short time window and very limited physical dimensions of a geofence warrant distinguish it from the multi-day, large-area nature of the data at issue in Carpenter.

The problems with the good faith exception

Regardless of whether the Supreme Court ends up siding with Chatrie or the government, a clear ruling can help ensure that future geofence cases avoid the concerning consequences of the good faith exception. Under that exception, as occurred in the Fifth Circuit in U.S. v. Smith and (up until now) in the Fourth Circuit in Chatrie, defendants can be prosecuted using evidence that courts expressly conclude was collected in violation of their constitutional rights.

In a recent law review article in the Georgetown Law Journal, Matthew Tokson and Michael Gentithes performed an empirical study showing (generally, not limited to cases specific to geofence warrants) that "courts frequently employ [the good faith exception] to avoid substantive constitutional rulings." Courts that invoke the good faith exception can choose to completely sidestep the question of constitutionality, since resolving that question will have no effect on the admissibility of the contested evidence. This leaves key constitutional questions unresolved, even as the number of cases raising them accumulates. The Supreme Court ruling in Chatrie has the potential to eliminate or—if the ruling's scope is unclear—at least reduce use by future courts of the good faith exception for geofence warrants.

Location tracking and the broader app ecosystem

It might be tempting to conclude that the entire geofence constitutionality question will become largely moot if Google does indeed complete its announced plan to migrate location data storage to personal devices. But there are many other companies that also collect and centrally store location data at least sporadically, and potentially constantly.

Consider, for example, providers of apps for fitness monitoring, tracking the location of family and friends, rideshare and food delivery services, and social media posts that include location tags. As long as location tracking

data exist in the hands of third parties, important questions of the associated Fourth Amendment protections will persist. And hopefully the court will consider that, while in some purely technical sense location data are "opt-in," in a practical sense, engaging in contemporary society requires not only a mobile phone, but also the use of apps that, in order to function, will sometimes need to collect location data.

What Are Geofence Warrants?

The MarkUp, By Leila Barghouty September 1, 2020

Location data on your smartphone is giving law enforcement new surveillance tools

Zachary McCoy went for a bike ride on a Friday in March 2019. The avid biker would do loops around his Gainesville, Fla., neighborhood and track his rides with a fitness app on his Android phone. McCoy didn't think anything unusual had happened that day. But months later, in January of this year, McCoy got an email from Google saying that his data was going to be released to local police. He'd become a potential suspect in a local burglary—and had no idea why.

"There was absolutely nothing that tied Zack to this at all, other than Google saying he was there on the street," McCoy's lawyer, Caleb Kenyon, said.

Police pegged McCoy as a potential suspect without security camera footage, eye-witness accounts, or any sort of forensic evidence because his device had shown up as near the burglary site. The Gainesville Police Department had gotten something called a geofence warrant granted by the Alachua County court.

Geofence warrants, or reverse-location warrants, are a fairly new concept.

With permission from a judge, they allow law enforcement to obtain anonymized data from Google from almost any device that was in a certain geographic area at a specific time. Police can then go back to Google for more specific user information on anyone they deem a suspect.

In McCoy's case, he was tracking his bike ride using Runkeeper, which makes use of Google's location services, just as many apps do. (Check your settings in your Google account—if "location history" is on, then Google has data on your movements.) He hired an attorney to fight the warrant before his personal information was released, and police ended up not pursuing the case. (The Gainesville Police Department declined to comment, except to say that there has not yet been an arrest in the burglary.)

Google is the only tech company publicly known to release this kind of information to law enforcement specifically in response to geofence warrants. It is not clear how many other companies do the same.

Microsoft assistant general counsel Hasan Ali, in an email response to The Markup's request for comment, said "Microsoft does not and would not be in a position to comply with any warrants seeking such information."

Apple and Facebook declined to comment on the record regarding the warrants and whether they have any similar data and do or do not provide it to law enforcement.

There's no centralized database or oversight of geofence warrants, so it's hard to measure exactly how often they're used and for what sorts of crimes. Criminal cases springing from such warrants have largely involved robberies, burglaries, and murders—but there's growing speculation that police may use them to gather information on people who attend protests.

According to The New York Times, federal law enforcement first used the warrants in 2016. Since then, local police departments have adopted the tool—and its use is growing rapidly.

In a court filing late last year, Google said law enforcement requests for geofenced location history data in its trove went up 1,500 percent between 2017 and 2018, and at least 500 percent between 2018 and 2019. Google has yet to release any exact figures, but reportedly they have received as many as 180 requests in a single week.

In an email response to The Markup's request for comment, Google's Director of Law Enforcement and Information Security, Richard Salgado, said, "We vigorously protect the privacy of our users while supporting the important work of law enforcement. We developed a process specifically for these requests that is designed to honor our legal obligations while narrowing the scope of data disclosed."

Civil liberties groups—and increasingly politicians and judges as well—are watching the rise in geofence warrants with concern. There are cases around the country challenging the constitutionality of such warrants, proposed legislation in New York to limit their use, and at least one member of Congress who believes the federal government should get involved.

"I think they're incredibly dangerous, particularly if there are not significant guardrails put in place," Rep. Kelly Armstrong (R-ND) told The Markup.

A traditional search warrant for a car or a house or a laptop typically targets a specific person police have probable cause to suspect of a crime.

Geofence warrants allow law enforcement officers to search when they don't have a potential suspect.

Geofencing itself simply means drawing a virtual border around a predefined geographical area. Data can then be gathered on users who enter that area.
Geofencing is often used by marketers trying to reach specific audiences. A conservative political organization called CatholicVote has used geofencing technology to identify Catholic church-goers and send targeted political ads to their devices. Clothing retailer Gap used the technology to send virtual ads to users within a certain distance of their physical ads. An NBC News report from late last year found that the University of North Carolina was using geofencing to monitor the location and social media activity of protesters on campus. And the American Civil Liberties Union found in 2016 that law enforcement was using a social media monitoring service called Geofeedia to track Black Lives Matter protesters.
(In response to the ACLU's report, Facebook, Twitter, and Instagram announced they would no longer provide their users' data to Geofeedia.)
While it's unclear exactly how deep police can dive into user data they obtain from geofence warrants, current cases where the warrants are being challenged are revelatory.
In an armed robbery case in Richmond, Va., police were able to use such a warrant to not only identify the accused but also access his location history from that day and personal information like his email address. That case is in federal court in the Eastern District of Virginia. In a burglary case in state court in San Francisco, a man was identified through a geofence warrant through which police also acquired two email addresses of his, a complete list of Google-associated applications he'd used, and the IP address of at least one of his devices.
(Defendants in both cases, which are wending their ways through court, argue that the warrants were unconstitutional.)
In a court filing in the Virginia case, Google said that in addition to location history, geofence warrants can include "account-identifying information" and "account subscriber information such as the Gmail address associated with the account and the first and last name entered by the user on the account."

Are These Warrants Constitutional?

Civil liberties groups say the issue with geofence warrants is just how much information from innocent individuals law enforcement can get their hands on.
The claim is that they violate the Fourth Amendment, which protects Americans against "unreasonable searches and seizures" and stipulates that warrants only be issued with probable cause "particularly describing the place to be searched, and the persons or things to be seized." The problem with geofence warrants is that the persons and place to be searched are rarely particular, and there's no limit to how many innocent people are included if they happen to be in law enforcement's search boundaries.
Police, on the other hand, generally argue that such warrants aren't so different from other types of surveillance—from using security camera footage to sifting through data from cell towers to see which devices passed through the area.
Google has not taken a public position on whether it believes the warrants are constitutional but says it does provide data when presented with a warrant. The company has outlined its process in court filings and said that it considers executing geofence warrants "a broad and intrusive search" that's significantly different from cellphone tower dumps.
The constitutional question is largely unsettled—no case involving a geofence warrant has made its way to a high-level court. But on Aug. 24, Magistrate Judge Gabriel A. Fuentes of the U.S. District Court for the Northern District of Illinois issued what is believed to be the first federal court opinion on the Fourth Amendment's relationship to geofence warrants.
Investigators in the state requested a geofence warrant three times in hopes of finding a suspect who allegedly stole prescription drugs. Despite repeatedly narrowing their request, Judge Fuentes declined to grant the warrant.
While geofence warrants are not in themselves "categorically unconstitutional," he wrote, investigators lacked probable cause to scoop up vast location data from cellphones of people who obviously had no connection to a crime but happened to be nearby when it was committed.
"The potential to use Google's capabilities to identify a wrongdoer by identifying everyone (or nearly everyone) at the time and place of a crime may be tempting," Fuentes wrote. "But if the government can identify that wrongdoer only by sifting through the identities of unknown innocent persons without probable cause and in a manner that allows officials to 'rummage where they please in order to see what turns up,' " then courts should not permit the practice.

There Are Political Efforts to Rein Them In

On April 8, state senator Zellnor Myrie introduced the Reverse Location Search Prohibition Act in New York.

The bill would prohibit "the search, with or without a warrant, of geolocation data of a group of people who are under no individual suspicion of having committed a crime, but rather are defined by having been at a given location at a given time."

If the bill passes, New York would become the first state where geofence warrants are banned.

"We can either create boundaries on what kinds of data companies can collect—only to be outpaced by new advances in technology—or we can put limits on how law enforcement can obtain and use that data," Myrie said in an email.

Armstrong, the North Dakota congressman, has also confronted Google about its compliance with geofence warrants.

At a hearing featuring the CEO's of Amazon, Apple, Facebook, and Google, Armstrong pointedly asked Google CEO Sundar Pichai about such warrants.

"People would be terrified to know that law enforcement could grab general warrants and get everyone's information everywhere," Armstrong said in the hearing. "It requires Congress to act, and it requires everybody that is a witness in this hearing to be willing to work too, because it is the single most important issue."

Pichai responded by saying Google thinks "it's an important area for Congress to have oversight" and that the company recently began automatically deleting location activity after "a certain period of time."

"I don't blame the tech companies solely for this," Armstrong told The Markup. "Congress's failure to act on this is going to become more and more of an issue."

A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet

Wired Magazine, by Mark Harris November 20, 2022

Google provided investigators with location data for more than 5,000 devices as part of the federal investigation into the attack on the US Capitol.

The FBI's biggest-ever investigation included the biggest-ever haul of phones from controversial geofence warrants, court records show. A filing in the case of one of the January 6 suspects, David Rhine, shows that Google initially identified 5,723 devices as being in or near the US Capitol during the riot. Only around 900 people have so far been charged with offenses relating to the siege.

The filing suggests that dozens of phones that were in airplane mode during the riot, or otherwise out of cell service, were caught up in the trawl. Nor could users erase their digital trails later. In fact, 37 people who attempted to delete their location data following the attacks were singled out by the FBI for greater scrutiny.

Geofence search warrants are intended to locate anyone in a given area using digital services. Because Google's Location History system is both powerful and widely used, the company is served about 10,000 geofence warrants in the US each year. Location History leverages GPS, Wi-Fi, and Bluetooth signals to pinpoint a phone within a few yards. Although the final location is still subject to some uncertainty, it is usually much more precise than triangulating signals from cell towers. Location History is turned off by default, but around a third of Google users switch it on, enabling services like real-time traffic prediction.

The geofence warrants served on Google shortly after the riot remained sealed. But lawyers for Rhine, a Washington man accused of various federal crimes on January 6, recently filed a motion to suppress the geofence evidence. The motion, which details the warrant's process and scale, was first reported by journalist Marcy Wheeler on her blog, Emptywheel.

In a statement, a Google spokesperson defended the company's handling of geofence warrants.

"We have a rigorous process for geofence warrants that is designed to protect the privacy of our users while supporting the important work of law enforcement," the company said. "When Google receives legal demands, we examine them closely for legal validity and constitutional concerns, including overbreadth, consistent with developing case law. If a request asks for too much information, we work to narrow it. We routinely push back on overbroad demands, including overbroad geofence demands, and in some cases, we object to producing any information at all."

Google requires a three-step process for geofence warrants to narrow their scope to only those most likely to be guilty of a crime. In the first and broadest step, the FBI asked Google to identify all devices in a 4-acre area, including the Capitol and its immediate surroundings, between 2 pm and 6:30 pm on January 6. Google initially found 5,653 active devices that "were or could have been" within the geofence at that time. When Google added in data from devices that only connected to its servers later that day, or the next, the number increased to 5,723. In the second step, the FBI asked Google for a list of devices that were present at the Capitol from 12 pm to 12:15 pm on January 6, and from 9 pm to 9:15 pm. As there were no rioters in the Capitol during those times, these devices likely belonged to congressional members or staff, police, and other people authorized to be there. Over 200 such phones were excluded from the initial list, reducing its total to 5,518.

For the final step, the government sought subscriber information, including phone numbers, Google accounts, and email addresses, for two groups of users. The first was for devices that appeared to have been entirely within the geofence, to about a 70 percent probability. The second was any devices for which the Location History was deleted between January 6 and January 13.

From this, in early May 2021, the FBI received identifying details for 1,535 users, as well as detailed maps showing how their phones moved through the Capitol and its grounds. Geofence evidence has so far been cited in over 100 charging documents from January 6. In nearly 50 cases, geofence data seems to have provided the initial identification of suspected rioters.

Rhine was first flagged to the FBI by tipsters who had heard that he had been inside the Capitol. But investigators only identified him in surveillance footage after they matched it against the precise geofence coordinates of his phone. His lawyer is now trying to get the geofence evidence thrown out on a number of grounds, including that it was overly broad in who it rounded up, and that Rhine had a constitutional expectation of privacy in his Google data.

"The government enlisted Google to search untold millions of unknown accounts in a massive fishing expedition," the attorneys wrote. "Just a small amount of Location History can identify individuals … engaged in personal and protected activities (such as exercising their rights under the First Amendment). And as a result, a geofence warrant almost always involves intrusion into constitutionally protected areas."

If the judge tosses the geofence evidence in the Rhine case, there is a chance that he and other suspects identified using it could walk free.

Opinion: Geofence warrants — the modern-day general warrant

Deseret News, By David Iglesias September 10, 2024

In a landmark decision on Aug. 9, the Fifth Circuit Court of Appeals declared that geofence warrants are unconstitutional under the Fourth Amendment, labeling them "modern-day general warrants." This ruling is not just a legal victory but a crucial affirmation of privacy rights in the digital age, arriving at a time when the use of such warrants by law enforcement is on the rise and concerns over digital surveillance are growing.

Geofence warrants, also known as reverse-location searches, allow law enforcement to collect location data from any device within a certain geographical area at a given time. The technique, which aims to identify suspects in criminal investigations, might seem like a perfect tool for catching criminals. However, it also represents a significant intrusion into the privacy of countless innocent people whose data is swept up in the process.

The Fifth Circuit's ruling comes as a direct contrast to a decision made by the Fourth Circuit Court of Appeals just a month earlier, which upheld the use of geofence warrants. This legal divide underscores the controversy surrounding this investigative technique and highlights the urgent need for clear regulations to protect Americans' privacy.

The statistics are alarming. Requests for geofence warrants have skyrocketed, with Google, the primary recipient of these requests, reporting a jump from 9,000 in 2019 to 11,500 in 2020. By 2021, geofence warrants constituted more than 25% of all warrant requests received by the tech giant. Despite the widespread use of this surveillance method, legislative action has been sparse. Utah remains the only state to have taken meaningful steps to regulate the use of geofence warrants, with the passage of HB57 in 2023. This law requires probable cause, a visual map of the geofence and annual reports on the use of such warrants, setting a standard for other states to follow.

Yet, as the Fifth Circuit's ruling demonstrates, even these measures may not go far enough. Judge James C. Ho, in his concurring opinion, eloquently reminded us of the Constitution's purpose: "Hamstringing the government is the whole point of our Constitution. ... Our decision today is not costless. But our rights are priceless."

His words serve as a powerful reminder that the Constitution was designed to protect citizens from government overreach, even in the face of potential costs to law enforcement efficiency.

Critics of the Fifth Circuit's decision argue that limiting the use of geofence warrants will hinder law enforcement's ability to solve crimes. However, this argument overlooks the fundamental principle that our rights are not negotiable. The erosion of privacy rights in the name of expedience sets a dangerous precedent, one that could lead to even greater intrusions on our freedoms in the future.

Furthermore, touting this as an "efficient" investigative practice in solving crime overlooks the harm that these virtual dragnets have already caused: Florida resident Zachary McCoy had to pull from his family's savings just to clear his name after the data from an exercise app he used for bike rides in his neighborhood turned him into a potential suspect for police investigating a burglary he knew nothing about. In Arizona, Jorge Molina was wrongfully arrested and defamed after police used a geofence warrant to investigate a drive-by shooting he wasn't involved in.

In an era where digital surveillance is becoming increasingly pervasive, the Fifth Circuit's decision is a crucial step in the right direction. It is a reminder that while technology may change, the fundamental rights enshrined in our

Constitution remain steadfast. As we move forward, it is essential that we continue to defend these rights, ensuring that the tools designed to protect us do not become instruments of oppression.
David Iglesias is a state government affairs associate at Libertas Institute.

A Model Framework for Regulating Geofence Warrants

Tech Policy Press, by Vivek Krishnamurthy June 9, 2025

Vivek Krishnamurthy is an Associate Professor of Law at the University of Colorado Law School and Director of its Samuelson-Glushko Technology Law and Policy Clinic.

In the United States, law enforcement's use of geofence warrants—court orders compelling tech companies to provide location data for all devices within a specified area and timeframe—is among the most contentious digital civil liberties issues of our time. Federal courts have struggled to apply existing Fourth Amendment doctrine to such searches, and in the meanwhile, a three-step procedure developed by Google—currently the main purveyor of location data to law enforcement—has been doing most of the work that the law should be doing in channeling how law enforcement agencies conduct searches of geolocation databases.

We believe that this situation is untenable, and that geofence searches should be regulated by statutory law. Since most crimes are state offenses and are investigated by state and local law enforcement, we believe that state legislatures should step up to improve the manner in which such searches are conducted. Accordingly, the Samuelson-Glushko Technology Law and Policy Clinic at the University of Colorado Law School has developed a comprehensive model policy framework that states can adopt to regulate these powerful but invasive investigative tools. We have done so at the request of the Center for Democracy and Technology (CDT), although the policy we have developed reflects the thinking of our clinic team, rather than the position of CDT, on this issue.

Geofence warrants represent a fundamental shift in how criminal investigations are conducted. Unlike traditional warrants targeting specific suspects, these "reverse-location warrants" cast a digital dragnet, capturing location data from every device within designated boundaries. When a bank robbery occurs, for instance, law enforcement might request data for all devices within a 150-meter radius during the hour surrounding the crime—potentially sweeping up information about hundreds of innocent bystanders.

The privacy implications of such warrants can be staggering. Location data reveals intimate details about our lives: where we work, worship, seek medical care, and our familial, recreational, and sexual associations. Yet confusion reigns in the federal courts as to the very constitutionality of such searches. Last year, the Fifth Circuit declared geofence warrants to be a species of a general warrant and therefore per se unconstitutional, but in April, a plurality of en banc Fourth Circuit justices found that geofence database queries did not even rise to the Fourth Amendment's definition of a search.

Our model policy addresses this uncertainty by establishing clear, technology-neutral guidelines that strongly protect privacy while recognizing the utility of this investigative tool—albeit only in rare and extenuating circumstances. The framework rests on four pillars:

In the United States, law enforcement's use of geofence warrants—court orders compelling tech companies to provide location data for all devices within a specified area and timeframe—is among the most contentious digital civil liberties issues of our time. Federal courts have struggled to apply existing Fourth Amendment doctrine to such searches, and in the meanwhile, a three-step procedure developed by Google—currently the main purveyor of location data to law enforcement—has been doing most of the work that the law should be doing in channeling how law enforcement agencies conduct searches of geolocation databases.

We believe that this situation is untenable, and that geofence searches should be regulated by statutory law. Since most crimes are state offenses and are investigated by state and local law enforcement, we believe that state legislatures should step up to improve the manner in which such searches are conducted. Accordingly, the Samuelson-Glushko Technology Law and Policy Clinic at the University of Colorado Law School has developed a comprehensive model policy framework that states can adopt to regulate these powerful but invasive investigative tools. We have done so at the request of the Center for Democracy and Technology (CDT), although the policy we have developed reflects the thinking of our clinic team, rather than the position of CDT, on this issue.

Geofence warrants represent a fundamental shift in how criminal investigations are conducted. Unlike traditional warrants targeting specific suspects, these "reverse-location warrants" cast a digital dragnet, capturing location data from every device within designated boundaries. When a bank robbery occurs, for instance, law enforcement might request data for all devices within a 150-meter radius during the hour surrounding the crime—potentially sweeping up information about hundreds of innocent bystanders.

The privacy implications of such warrants can be staggering. Location data reveals intimate details about our lives: where we work, worship, seek medical care, and our familial, recreational, and sexual associations. Yet confusion reigns in the federal courts as to the very constitutionality of such searches. Last year, the Fifth Circuit declared

geofence warrants to be a species of a general warrant and therefore per se unconstitutional, but in April, a plurality of en banc Fourth Circuit justices found that geofence database queries did not even rise to the Fourth Amendment's definition of a search.

Our model policy addresses this uncertainty by establishing clear, technology-neutral guidelines that strongly protect privacy while recognizing the utility of this investigative tool—albeit only in rare and extenuating circumstances. The framework rests on four pillars:

First, strict limitations on when geofence warrants may be used. These warrants should be reserved for investigating only the most serious crimes—typically those involving violence or severe harm. States can define eligible offenses using their existing classifications for the most serious felonies or by referencing crimes that qualify for wiretap warrants.

Second, robust exhaustion requirements. Before seeking a geofence warrant, law enforcement must demonstrate that traditional investigative methods—witness interviews, surveillance footage, targeted suspect tracking—have either failed or would likely prove futile. This prevents premature use of privacy-invasive investigative techniques when less invasive alternatives exist.

Third, enhanced judicial oversight throughout the process. Our framework introduces a four-step process that begins with law enforcement obtaining a count of devices within their proposed geofence via subpoena. This innovation helps assess whether the number of devices for which location data will be collected is reasonable under the circumstances. The policy then implements escalating legal standards at each stage: probable cause for initial anonymized data, an intermediate standard for expanded temporal searches, and renewed probable cause for de-anonymization. Courts remain actively involved throughout, preventing the current practice where a single warrant authorizes the entire process.

Fourth, careful tailoring factors to minimize privacy intrusions. Judges must consider the geographic scope, timeframe, population density, and presence of sensitive locations like health clinics or houses of worship. A geofence warrant covering Times Square on New Year's Eve demands far greater scrutiny than one targeting a remote rural area. These factors ensure searches remain as narrow as possible while still serving investigative purposes.

The policy also mandates transparency through annual reporting requirements similar to those governing wiretaps. This creates public accountability for how often geofence warrants are used, their success rates, and how many innocent people's data is collected.

Importantly, our framework anticipates technological change. With Google transitioning its Location History feature to on-device storage later this month, law enforcement will likely pivot to other data sources—mobile carriers, app developers, and data brokers—when issuing geofence warrants. Our technology-neutral approach ensures protections remain effective regardless of which entities hold location data.

Our proposal is not about hampering legitimate investigations into serious crimes. When traditional methods fail to identify suspects, geofence warrants can provide crucial leads. But their invasiveness demands that they are used only as a last resort, and subject to strong safeguards to protect the privacy of innocent individuals who just happen to be in the vicinity of where a serious crime has been committed.

As location-tracking technology becomes ever more pervasive and precise, the need for state action to govern geofence warrants has never been more urgent. Courts move slowly, deciding individual cases without establishing comprehensive rules that govern the process by which search warrants are issued and executed. Legislation can provide the clarity law enforcement needs while protecting citizens' reasonable expectation of privacy in their movements.

The Fourth Amendment (Common Interpretation)

National Constitution Center, by Barry Friedmand and Orrin Kerr

Imagine you're driving a car, and a police officer spots you and pulls you over for speeding. He orders you out of the car. Maybe he wants to place you under arrest. Or maybe he wants to search your car for evidence of a crime. Can the officer do that?

The Fourth Amendment is the part of the Constitution that gives the answer. According to the Fourth Amendment, the people have a right "to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." This right limits the power of the police to seize and search people, their property, and their homes.

The Fourth Amendment is often in the news. Police in some cities have engaged in aggressive use of "stop and frisk." In some cases, a police stop ends with officers or others firing their weapons. There is concern about the use of aerial surveillance, whether by piloted aircraft or drones. And AI algorithms are being used to mine data looking for suspicious activity.

The application of the Fourth Amendment to all these activities would have surprised those who drafted it, and not only because they could not imagine modern technologies like the Internet and drones. They also were not familiar with organized police forces like we have today. Policing in the eighteenth and early nineteenth centuries was a responsibility of the citizenry, which participated in "night watches." Other than that, there was only a loose collection of sheriffs and constables, who lacked the tools to maintain order as the police do today.

The primary concerns of the generation that ratified the Fourth Amendment were "general warrants" and "writs of assistance.". In England, the King employed "general warrants" to go after his political enemies, leading to the famous decisions in Wilkes v. Wood (1763) and Entick v. Carrington (1765). General warrants allowed the King's messengers to break into the homes of the King's critics and arrest them without probable cause that they had committed a crime. In those cases, judges decided that general warrants were illegal. Over in the colonies, the King's officials used the writs of assistance—like general warrants, but often unbounded by time restraints—to search for goods on which taxes had not been paid. James Otis famously challenged the writs in a Boston court. Although he lost, some such as John Adams attribute this legal battle as the spark that led to the Revolutionary War. Both controversies helped support the idea that a person's home is their castle, not easily invaded by the government.

Today the Fourth Amendment is understood as placing limits on the government whenever it detains or searches a person or property. The Fourth Amendment also provides that "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 idea is that to avoid the evils of general warrants, each search or seizure should be cleared in advance by a judge, and that to get a warrant the government must show "probable cause"—a certain level of suspicion of criminal activity—to justify the search or seizure.

The government can conduct a legal search if it has a valid warrant or else an exception to the warrant requirement applies. Police can search cars without warrants, they can detain people on the street without them, and they can always search or seize in an emergency without going to a judge.

The Fourth Amendment usually comes in court during a criminal prosecution. The Supreme Court has ruled that if the police seize evidence as part of an illegal search, the evidence normally cannot be admitted into court. This is called the "exclusionary rule." It is controversial because in most cases evidence is being tossed out even though it shows the person is guilty and, as a result of the police conduct, they might avoid conviction. "The criminal is to go free because the constable has blundered," declared Benjamin Cardozo (a famous judge and ultimately Supreme Court justice). But, responded another Supreme Court justice, Louis Brandeis, "If the government becomes the lawbreaker, it breeds contempt for the law."

One of the difficult questions today is what constitutes a "search"? If the police standing in Times Square in New York watched a person planting a bomb in plain daylight, we would not think they needed a warrant or any cause. But what about installing closed circuit TV cameras on poles, or flying drones over backyards, or gathering evidence that you have given to a third party such as an Internet provider or a banker?

Another hard question is when a search is acceptable when the government has no suspicion that a person has done something wrong. Lest the answer seem to be "never," think of airport security. Surely it is okay for the government to screen people getting on airplanes, yet the idea is as much to deter people from bringing weapons as it is to catch them—there is no "cause," probable or otherwise, to think anyone has done anything wrong. This is the same sort of issue with bulk data collection, and possibly with gathering biometric information.

Whatever the right answers are, advancing technology and the many threats that face society means that the Fourth Amendment will continue to play a central role in the future.

United States Constitution, Fourth Amendment

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.