4-29-2021

Geofence Warrants: An Attack on the Fourth Amendment

Golden Gate University School of Law

GGU Law Review Blog

APRIL 29, 2021 NO COMMENTS

Geofence Warrants: An Attack on the Fourth Amendment

Introduction to Geofence Warrants

Photo by Roberto Catarinicchia on Unsplash.

Imagine a world where a king could compel the search of anybody, anywhere, and for anything. This world inspired James Madison to draft the Fourth Amendment, and is also a world we are returning to. The Fourth Amendment was created to protect against indiscriminate general warrants used in Georgian England, which subjected colonists to unrestricted invasions of privacy. Today, these general warrants come with a new name and in a new form: geofence warrants. Geofence warrants permit law enforcement to obtain the location data of every person that was in a specific geographic area where a crime occurred, in an effort to work backwards and identify the culprit. Essentially, the days have returned in which all the King's horses and all the King's men can burst into every apartment in a building to find their suspect.

The Fourth Amendment of the United States Constitution protects the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. In general, a warrant is required for searches and seizures of things and places in which people have a reasonable expectation of privacy. In a 2018

landmark decision, *Carpenter v. United States*,138 S. Ct. 2206 (2018), the United States Supreme Court ruled that people have a legitimate, reasonable expectation of privacy in cell-site location information (CLSI), and therefore, warrants are required for dissemination of CSLI to law enforcement. CLSI, the information sought by law enforcement when employing geofencing techniques in an investigation, is geolocation data generated by a cell phone's communication with nearby cell towers.

In *Carpenter*, the defendant, a suspect in a series of robberies, challenged the constitutionality of law enforcement's warrantless acquisition of the defendant's CSLI. The government obtained 12,898 location points cataloging the defendant's movements over 127 days. The defendant argued that the constant location records generated by CSLI raise enough privacy concerns as to implicate the Fourth Amendment. The government compared its use of CSLI to tracking vehicles with GPS.

In its opinion, the Supreme Court explained that historical CSLI records present even greater privacy concerns than for GPS monitors. A cell phone is almost a "feature of human anatomy," that tracks almost the exact movements of its owner. A cell phone, unlike a gps, follows its owner into "private residences, doctor's offices, political headquarters, and other potentially revealing locales." The Supreme Court compared tracking the location of a cell phone to attaching an ankle monitor to the phone's user and described this tracking as "near perfect surveillance." The Court held that people have a reasonable expectation of privacy in their CSLI, reinforcing that "a person does not surrender all Fourth Amendment protection by venturing into the public sphere."

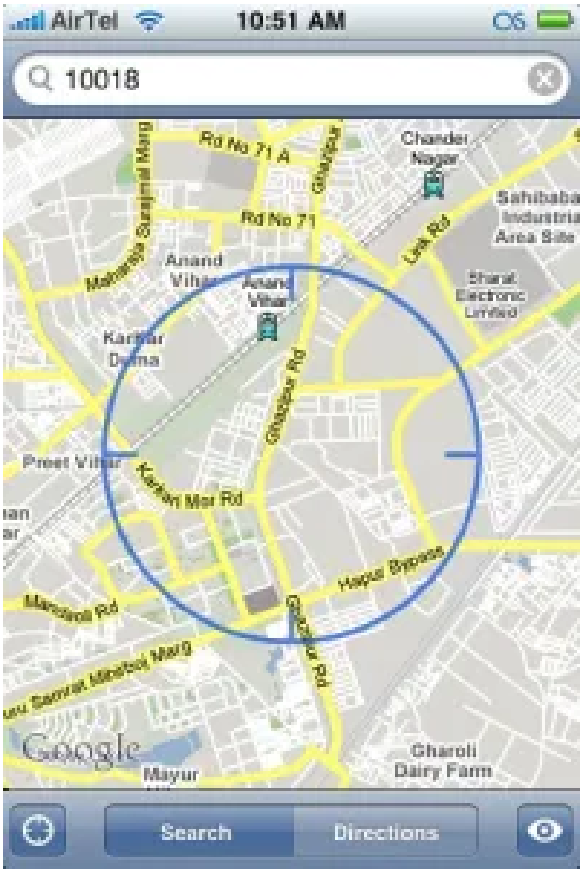

Photo by Amit Gupta on Flickr.

Constitutional Problems With Geofence Warrants

Geofence warrants do not pass the requirements of constitutional muster and therefore should not be honored. The keystone of the Fourth Amendment, which protects against unreasonable searches and seizures, is reasonableness. Generally, notwithstanding a few historical exceptions, a proper warrant makes a search reasonable. A warrant must be issued upon probable cause, supported by oath and affirmation by a neutral magistrate, with a particular description of where to search and what to be seized. In relevant part, it is questionable whether geofence warrants, due to the sweeping amount of information they generate, satisfy the particularity requirement of the Fourth Amendment.

Photo by Steven Nichols on Flickr.

The particularity requirement of the Fourth Amendment acts to limit the scope of a search, and to prevent the reviled general warrants of old. When it comes to geofence warrants, a clear policy of what data is protected by the Fourth Amendment and what data is fair game has not been established. Unlike traditional warrants that identify a suspect prior to an issuance of a warrant, geofence warrants collect from every and any device in a certain geographical location, in an effort to catch their unknown suspect. Law enforcement casts a large net that may contain their suspect, and then sifts through those results to find their catch.

It has been argued that geofence warrants inherently violate the particularity requirement because they fail to identify a single individual suspected of a criminal offense. In *U.S. v. Chatrie*,Dkt. No. 3:19-cr-00130 (E.D. Va.), the gunman in an armed bank robbery held a cell phone up to his ear, which the government used as justification for a geofence warrant. This resulted in the dissemination of Google location data from 19 cell phones that were in the geographic area of the bank during the robbery. To satisfy the Fourth Amendment, the government used a multi-step, pseudonymized process to compel location information from Google. Law enforcement then sifted through this pseudonymized list and flagged certain "suspicious" profiles to get more specific information.

However, in *In re Search of Information Stored at Premises Controlled by Google*, an Illinois District Court rejected the issuance of a geofence warrant on grounds of particularity. There, law enforcement attempted to identify an unknown suspect through the results of a geofence warrant application for Google location data on "all the data of the cellular telephones that accessed Google applications or used Google's operating system" in three locations. The Court rejected the geofence warrant application, holding that it was not narrowly tailored, and that the pseudonymization process was "devoid of any meaningful limitation." The Court held that it was problematic that the geofence warrant sought to gather evidence of all phone users in the particular geographic location, when there was only evidence that one user committed a crime.

The Ramifications of Geofencing For The Innocent

Despite these unresolved issues of constitutionality, some people may still feel that they have nothing to hide. However, those who believe they have nothing to hide should be nonetheless concerned. Real consequences to innocent people have resulted from geofence warrants. One such incident involves Zachary McCoy, an innocent bicyclist in Gainesville, Florida. In 2019, McCoy was out for a routine bike ride in his neighborhood and was tracking his ride with an app that recorded his route on his Google account. McCoy ended up passing by a particular house three times, which also happened to be the victim of a burglary that day. Almost a year later, McCoy was notified by Google that local law enforcement, via a geofence warrant, was requesting his account information, and that he had seven days to block the request. Only supplied with a case number, McCoy searched the police department's website to figure out what he was mixed up in, and eventually hired an attorney to clear his name of wrongdoing. McCoy's use of an app to track his mileage during a bike ride turned into a scary scenario putting his freedom and privacy at risk, that also required time and money to resolve.

Photo by Hege on Flickr.

However, McCoy's problems were relatively trivial compared to what befell Jorge Molina, a resident of Avondale, Arizona, in 2018. After a week of investigating a murder with no leads, Avondale law enforcement drafted a geofence warrant to Google. The warrant application requested information on all devices that were in the geographic location of the murder, at the time of the murder. Four Google accounts were given to the Avondale Police, including Jorge Molina's. Police quickly realized that a device logged into Molina's Google account was in the area of the murder at the time of the murder. Additionally, Molina was the owner of a white Honda, the same car description as used in the murder.

Avondale Police arrested Molina at a Macy's warehouse where he worked, and he spent six days in jail. Turns out, Molina's stepfather was using one of Molina's old phones, and his car, to carry out the murder. Even though Molina was released, his life was permanently altered. He spent six days in jail, he lost his job, and he lost his car because it was impounded and repossessed because he had no income. Furthermore, he had to drop out of school for missing too many classes, and he regularly has nightmares about the police and his time in jail.

Geofence warrants are a reincarnation of the reviled general warrants so detested by our founding fathers. They make a mockery of our Fourth Amendment rights and allow for the invasion of every person's personal privacy. The search of every person's pockets in Golden Gate Park in response to a robbery would not be permitted. Neither should a search of every person's whereabouts via their phone, just for the off chance that law enforcement stumbles upon their culprit.

smcadoppi

In this area you can display your biographic info. Just visit *Users > Your Profile > Biographic info*

Leave a Reply

Enter your comment here...

Search blog