Are Geofence Warrants Constitutional

By Paul Engel

May 9, 2023

- Under what circumstances can a government actor legally search cellphone location data?
- What are the requirements for a legitimate geofence warrant.
- Can this case out of California help turn the tide in our dissent into tyranny?

Most of us are aware that generally law enforcement needs to get a warrant before searching our property. Recent advances in technology, however have made the distinctions for the necessity of a warrant more and more difficult. For example, can law enforcement search for cellphone data within an area for their criminal investigations? Are these geofence warrants a violation of the Fourth Amendment's requirement that warrants be issued only when there is probable cause and specifically stating the places to be searched and the things to be seized? A recent case heard in the California Court of Appeals looks to answer that very question.

For those of you who may not be familiar with the term, a geofence warrant is a request, generally by law enforcement, for the location data for all devices within a defined area during a defined time. Think of the mapping software so many of us use. Imagine you're looking for a place to meet up with friends for lunch. You put a marker in the general area you want to meet, then ask the software for a list of restaurants

within 10 miles of that location. You have created a geofence (the within 10 miles of your selected location), and you are asking for a list of known restaurants within that geofenced area. Now imagine law enforcement places their own marker near the scene of a crime or other place of interest, and they want a list of all of the cellphones within a certain distance of that marker for a timeframe related to a crime. Now, instead of using mapping software, they reach out to one of the many tech companies that collect location data from the apps on your phone for that list. That request would come in the form of a geofence warrant, meaning a judge would have to look at the request and determine if it meets all the requirements listed in the Fourth Amendment.

People v. Meza

A case recently heard by the California Court of Appeals challenged the constitutionality of these geofence warrants.

Los Angeles County Sheriff's Detective Jonathan Bailey applied for a search warrant directing Google to identify individuals whose location history data indicated they were in the vicinity of the six locations visited by Thabet on March 1, 2019.

People v. Meza

First, we need to understand what is required under the Fourth Amendment before a warrant can be issued.

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.

U.S. Constitution, Amendment IV

We have a right to be secure from unreasonable searches and seizures. That's why the government has to meet the requirements of the Fourth Amendment before they can search or seize your person, house, papers, or effects. Those requirements are:

- They must show probable cause.
    - Apparent facts discovered through logical inquiry that would lead a reasonably intelligent and prudent person to believe that an accused person has committed a crime, thereby warranting his or her prosecution, or that a Cause of Action has accrued, justifying a civil lawsuit. – Probable Cause – The Free Legal Dictionary
- A particular description of the places to be search.
- A particular description of the things to be seized.

The six locations were chosen by Detective Bailey after video surveillance identified them as places Mr. Thabet had visited before his murder. As part of the application process for requesting a warrant, the requester must provide an affidavit showing probable cause.

In an affidavit supporting the application, Bailey described Thabet's murder as seen on the surveillance footage of the bank parking lot. Bailey stated he had viewed surveillance camera footage from several of the other locations Thabet had visited that morning and had seen the gray and red sedans in the footage.

People v. Meza

Next, the warrant request listed the six locations along with the area around each location for the geofence to be established and the timeframes for which Detective Bailey was requesting data. The warrant established a three-step process by which Google (the owners of the database to be searched) would provide the requested data.

At step one, Google was directed to search location history data for the six designated locations and times and produce an anonymized list of devices found within the search areas in the designated timeframes, including the individual times each device was recorded in the search area during the applicable time period.

At step two, law enforcement would review the anonymized list of devices "to remove devices that are not relevant to the investigation, for example, devices that were not in the location for a sufficient period of time." If law enforcement believed additional information was needed to determine whether a particular device was relevant to the investigation, law enforcement could request that Google provide additional location history information for that device even if that information fell outside of the initial geographic and temporal search parameters.

At step three, law enforcement could demand identifying information from Google for all devices law enforcement deemed relevant to the investigation. The warrant directed Google to provide this identifying information without additional legal process.

People v. Meza

Based on the information collected by this geofence warrant, Daniel Meza and Walter Meneses were identified as suspects. At trial they moved to have the geofence warrant quashed and suppress the evidence related to it, but their motions were denied. Daniel Meza plead guilty to first degree murder and Walter Meneses plead no contest to second degree murder.

On appeal Meza and Meneses contend the trial court erred in denying their motion to suppress, arguing the geofence warrant violated their rights under the Fourth and Fourteenth Amendments to the United States Constitution and did not comply with the California Electronic Communications Privacy

Act of 2016 (Pen. Code, § 1546 et seq.)4 (CalECPA).

People v. Meza

Though California Court of Appeals found that the geofence warrant used in this case did not violate CalECPA, they did find it violated the Fourth Amendment, specifically the particularity requirement.

The Details Matter

When it comes to warrants, not only do the details matter, but they especially matter when it comes to the particularity of the places to be searched and the things to be seized.

A search is presumptively reasonable, and thus in compliance with the Fourth Amendment, if supported by a warrant describing with particularity the thing or the place to be searched. (See People v. Weiss (1999) 20 Cal.4th 1073, 1082.) "'The manifest purpose of this particularity requirement [is] to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.'" (People v. Amador (2000) 24 Cal.4th 387, 392; accord, Maryland v. Garrison (1987) 480 U.S. 79, 84.)

People v. Meza

The reason why the Constitution is so picky about the particularity requirement for warrants is the colonists' history with general warrants and specifically with writs of assistance. These were warrants that allowed British officials to search without any probable cause, then if the found any contraband, fill in the warrant with the specifics of the charge. Hence, the three part requirement for warrants in the Fourth Amendment. The first requirement looked at by the court

was probable cause.

Meza and Meneses contend Detective Bailey's assertion of probable cause in his affidavit was insufficient because "[t]here was absolutely no evidence that either suspect had, or was using, a phone or other device at any time during the relevant timeframe."

Probable cause does not require conclusive evidence that a search will uncover relevant evidence, only that "'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'"

It was reasonable for the magistrate to conclude the perpetrators were carrying cell phones the morning of the murder and used them in coordinating their movements.

People v. Meza

It was quite reasonable to believe that the perpetrators of the murder were carrying cellphones at the time, so there was probable cause to believe that their location data would not only show them at the scene of the crime, but following the victim to that location.

Next, the court looked at the particularity of the search.

The warrant in this case sufficiently described the place to be searched (Google's database of users' location history) and the items to be retrieved from that search (designated records for users found within the boundaries of certain coordinates at certain times). Indeed, Mesa and Meneses do not argue there was any ambiguity in the warrant that would lead law enforcement or Google personnel to search an incorrect database or to identify individuals not contemplated by the text of the warrant.

However, the warrant here failed to meet the particularity requirement because it provided law enforcement with unbridled

discretion regarding whether or how to narrow the initial list of users identified by Google.

People v. Meza

The court based this decision on what law enforcement could do with the data once it was collected.

Once the step one search had been conducted, law enforcement officials were able to enlarge the geographic parameters of the search and request additional information on any of the potentially thousands of users identified without any objective criteria limiting their discretion. Again, at step three law enforcement could seek identifying information of any of the users found within the search parameters without restriction on how many users could be identified or any further showing that information concerning each individual user would be relevant to the case.

People v. Meza

The court identified two issues with the particularity of the warrant. Once the initial data was collected, law enforcement could request additional information without any limitations on anyone who happened to be in that area. There was no requirement to show probable cause that the person they would request additional information on had anything to do with the crime being investigated. Furthermore, the court was concerned about how many people law enforcement wanted identifying information on. That doesn't bother me nearly as much as the other issue the court identified: That law enforcement did not need to provide probable cause that the individual user was relevant to the case. In other words, once they were swept up in the geofence warrant, there was no requirement that there had to be probable cause that the individual was involved before law enforcement could collect data about them. This problem was further exacerbated by the breadth of the warrant.

In determining whether a warrant is overbroad courts consider

"whether probable cause existed to seize all items of a category described in the warrant" and "whether the government could have described the items more particularly in light of the information available to it at the time the warrant issued."

The geofence warrant in this case ran afoul of both of these requirements. First, the warrant authorized the identification of any individual within six large search areas without any particularized probable cause as to each person or their location. For example, the first search location, the area around Thabet's apartment complex, allowed law enforcement to obtain information on every individual in a seven-and-a-half-acre area over a 75 minute period in the early morning. The search area included Thabet's entire apartment complex and surrounding buildings despite the lack of any evidence (or supported inference) that the suspects left their vehicles, let alone entered the apartment building.

Second, law enforcement officials failed to draw the search boundaries as narrowly as they could have given the information available. …

The timeframes designated in the geofence warrant were also not narrowly tailored.

People v. Meza

What we have here is the law enforcement equivalent of a dragnet, pulling in the information for everyone in these areas, hoping that they would "throw back" those that were not of interest in this case. Sounds awfully close to the writs of assistance I described earlier.

All of this led the court to find that the warrant was unconstitutional, although they did leave in place the convictions of both Meza and Meneses.

Conclusion

It’s important to remember that although this court came to a decision based on the Constitution of the United States, this was a court of the State of California. Therefore its opinion is only binding on the parties to the case and the precedent within that state. The case does, however, make two interesting constitutional points.

First, this court upheld the Supremacy Clause of the Constitution.

This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.

U.S. Constitution, Article VI, Clause 2

So, even though the warrant did not violate California law, it did violate the Constitution of the United States. Not only did the judges support the supremacy of the Constitution, but they showed themselves bound to it, even if the laws of California were at odds with it. This case also pointed out a couple of fundamental flaws in the geofence warrant process, which is most likely replicated across the nation.

For a warrant to be valid, it must particularly describe what is to be searched and what is to be seized. While many may point out that these warrants do particularly describe where the data to be searched is, they may not particularly describe what data for which they are searching. This is why judges need to make sure that any geofence warrant is limiting both the size and timeframe to gather the particular data needed. Once the anonymous data has been searched and specific details requested, there must again be probable cause before the identifiable details are released. In my mind, this would require an additional warrant, making sure that law

enforcement provides, under oath, both the probable cause for why the data is needed and the specific details of what they are requesting.

I hope anyone who is aware of a case where someone has been caught up in an overly broad and insufficient warrant, will share this information with the individual and their legal team. This case may be an early step in reigning in government collusion with big tech to spy on the American people.

E-Mail Paul Engel: paul@constitutionstudy.com