Geofencing Warrants

Author : Jeff Welty

Categories : Search and Seizure, Uncategorized

Tagged as : digital evidence, fourth amendment, geofencing, location, Search and Seizure, search warrants, wral

Date : July 30, 2019

WRAL has several stories up about geofencing warrants. One major article is here. It describes a search warrant obtained by the Raleigh Police Department in a murder case. The warrant ordered "Google [to] hand over the locations of every [mobile] device within the confines of [a defined geographic area] during a specified time period." In a nutshell, the police were trying to figure out who was near the scene of the crime when the murder took place and asked Google to comb its data banks to find out. This post is intended to start a conversation about warrants of this kind.

How geofencing works. As it pertains to law enforcement, geofencing begins with officers defining an area of interest and a time period. The size of the area may vary. This Gizmodo story states that it ranges "from tiny spaces to larger areas covering multiple blocks," while the warrant in WRAL's recent story encompassed "nearly 50 acres." The amount of time covered by such warrants is also not uniform. The warrant in WRAL's story was for less than an hour, but Minnesota Public Radio reported here on a similar warrant that encompassed "every cellphone in [a] dense, urban area[] . . . over a 33-hour window."

Officers then seek a warrant requiring Google to provide information about any devices in the specified location during the specified time. Google has a database called SensorVault that contains enormous amounts of user location information, which it collects in a variety of ways. WRAL explains that "[d]evices that run Google's Android operating system – and even Apple products that users connect to Google through Gmail or Maps – collect locations by default." Sometimes the location data is GPS-based and very accurate, as when a user has enabled location services to be able to use Google Maps most conveniently. For other users, the location information may be based on cell tower location or connection to a particular wifi network, and so may be less precise.

Google doesn't collect this data to help law enforcement, of course. It uses the location information to sell advertising. Perhaps ironically, the business side of WRAL's operation advertises geofencing as a way for advertisers to "target" people who frequent competing businesses. For example, "Leith Cars can fence all of the car dealerships and car repair shops in the Triangle to capture potential car shoppers on other car lots." And "Carolina Ale House can fence Mellow Mushroom, Longhorn Steakhouse and TGI Fridays to capture their competitors' frequent visitors." When a Mellow Mushroom customer visits WRAL's website, the site, with Google's help, can serve up ads for Carolina Ale House.

But back to warrants. When a warrant is issued and served on Google, Google provides responsive data. According to WRAL, it does so using a "multi-step process." Initially, Google doesn't provide "actual device information" but only "anonymized 'device IDs.'" Officers must then "narrow down and resubmit to Google for actual account information." I don't understand exactly what that means, but perhaps Google will provide account information for only a few devices that become of interest based on cross-referencing the geofencing dataset against other evidence. For example, in a case that involves a series of crimes, perhaps officers can ask Google to unmask devices that appear in multiple geofencing datasets as those devices are more likely to be associated with perpetrators.

The law of geofencing. As of this writing, there are zero cases on Westlaw, anywhere in the country, that include the terms "search warrant" and "geofenc!" in the same paragraph. Likewise, there is virtually no secondary source material about these warrants. Yet at least eight geofencing warrants have issued in Wake County alone, and nearly

two dozen have been obtained in a single county in Minnesota. No one but Google seems to know how many have been issued nationally, and Google isn't saying: its transparency report doesn't break out this type of warrant separately. As usual with digital evidence, law enforcement officers are on the cutting edge while courts struggle to keep up.

Absent any legal authority, what follows is my preliminary thinking about geofencing warrants.

First, it isn't clear that a search warrant is legally required to obtain geofencing information. The Supreme Court ruled in *Carpenter v. United States,* __ U.S. __, 138 S.Ct. 2206 (2018), that law enforcement conducts a search under the Fourth Amendment when it collects cell site location information about an individual, covering an extended period of time, from a service provider. The Court stated that a warrant is normally required to access such information. Although not all the information in SensorVault is cell site location information, it is all location data and I would expect extended tracking using SensorVault data to be viewed in much the same way as cell site location information. However, as I noted in my post on *Carpenter*, a footnote in the opinion reserves the question "whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be." Short-term tracking is less intrusive than the weeks-long tracking that was at issue in *Carpenter.* It is closer to what law enforcement officers might do using traditional surveillance techniques. Geofencing warrants, with their short time frames, squarely present the question whether a warrant is required to obtain short-term location data from a private company.

Even if Google *could* provide law enforcement with geofencing data without a warrant, though, it *doesn't.* As a matter of company policy, it requires a search warrant. So the question about whether a warrant is necessary may take a backseat to the question of whether and when a judicial official should issue a geofencing warrant.

Search warrants require probable cause and particularity. Normally, law enforcement officers apply for a search warrant when they have good reason to believe that a particular person has committed a particular crime and that the warrant will uncover evidence thereof. Officers presumably could seek SensorVault data in such a case: officers could obtain an order that Google produce any data connecting a suspect's device with a particular time and place. I can see no legal quibble with that. However, law enforcement appears to turn to SensorVault mainly when officers do not have an individual suspect. There may be probable cause that the pepetrator's device will be recorded in SensorVault, but law enforcement doesn't know who the perpetrator is at that point, and is asking Google to provide data on dozens or hundreds of individuals, most of whom are not guilty of anything.

In that way, geofencing warrants are similar to warrants for cell tower dumps, where law enforcement seeks information about all the cell phones that contacted a tower near a crime scene around the time the crime was committed. Unfortunately, the legal status of tower dumps is also unclear. Some contend that tower dumps "sweep so broadly that they amount to unconstitutional general warrants." Michael Price et al., *Building on Carpenter: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider*, The Champion (Dec. 2018). Most pre-*Carpenter* cases disagreed, holding not only that tower dumps are permissible with a warrant, but also that they may be conducted without a warrant, because they seek only provider records in which subscribers have no reasonable expectation of privacy under the third-party doctrine. It isn't clear whether that reasoning survives *Carpenter* – again, the Supreme Court expressly declined to consider tower dumps. But at least a couple of post-*Carpenter* cases have held that tower dumps are permissible under the Fourth Amendment with a warrant. *See, e.g., United States v. James,* 2018 WL 6566000 (D. Minn. Nov. 26, 2018) (holding that tower dump warrants were supported by probable cause where "there was a fair probability that data from the cellular towers in the area of the crimes would include cellular data related to the individual responsible for the robberies being investigated, and that by cross-referencing the data, that individual could be identified," and ruling that warrants did not lack particularity as "the warrant applications seek information that is constrained—both geographically and temporally—to the robberies under investigation," even though not limited to a single suspect). Perhaps courts will view geofencing warrants the same way – permissible with a warrant, at least for a short enough period of time and a small enough area.

Further reading and concluding thoughts. Additional WRAL stories are here and here. One of the search warrants that is the subject of WRAL's reporting is here. A related *New York Times* story, behind its paywall, is here. A *Slate* story is here.

I mentioned at the outset that I hope that this post starts a conversation. I really would like to crowdsource insights about this topic. This is new subject matter to me and I may have basic facts wrong. Even if I have the facts mostly right, the technology raises significant legal questions that don't have obvious answers. If you have any experience with this technology, with these warrants, or have thoughts about the proper resolution of these legal issues, please weigh in.