Google's 'SensorVault' Tracks Your Movements for Past 10 years

by Jennifer Lynch via darcy - EFF *Sunday, Apr 28 2019, 10:38pm*
international / prose / post

> Do you know exactly where you were five years ago? Did you have an Android phone at the time? It turns out Google might know—and it might be telling law enforcement.

In a new article, the New York Times details a little-known technique increasingly used by law enforcement to figure out everyone who might have been within certain geographic areas during specific time periods in the past. The technique relies on detailed location data collected by Google from most Android devices as well as iPhones and iPads that have Google Maps and other apps installed. This data resides in a Google-maintained database called “Sensorvault,” and because Google stores this data indefinitely, Sensorvault “includes detailed location records involving at least hundreds of millions of devices worldwide and dating back nearly a decade.”

The data Google is turning over to law enforcement is so precise that one deputy police chief said it “shows the whole pattern of life.” It’s collected even when people aren’t making calls or using apps, which means it can be even more detailed than data generated by cell towers.

The location data comes from GPS signals, cellphone towers, nearby Wi-Fi devices and Bluetooth beacons. According to Google, users opt in to collection of the location data stored in Sensorvault. However, Google makes it very hard to resist opting in, and many users may not understand that they have done so. Also, Android devices collect lots of other location data by default, and it’s extremely difficult to opt out of that collection.

Using a single warrant—often called a “geo-fence” or “reverse location” warrant—police are able to access location data from dozens to hundreds of devices—devices that are linked to real people, many of whom (and perhaps in some cases all of whom) have no tie to criminal activity and have provided no reason for suspicion. The warrants cover geographic areas ranging from single buildings to multiple blocks, and time periods ranging from a few hours to a week.

So far, according to the Times and other outlets, this technique is being used by the FBI and police departments in Arizona, North Carolina, California, Florida, Minnesota, Maine, and Washington, although there may be other agencies using it across the country. But police aren’t limiting the use of the technique to egregious or violent crimes—Minnesota Public Radio reported the technique has been used to try to identify suspects who stole a pickup truck and, separately, $650 worth of tires. Google is getting up to 180 requests a week for data and is, apparently, struggling to keep up with the demand.

Law enforcement appears to be seeking warrants to access this extremely detailed location data. However, it’s questionable whether the affidavits supporting those warrants truly establish probable cause and also questionable whether judges fully understand what they’re authorizing when issuing

these warrants.

According to the Times, the warrants frequently rely on an officer's assertion that the fact that "Americans owned cellphones and that Google held location data on many of these phones" somehow supports probable cause for the warrant. The warrants also list GPS coordinates that supposedly "geo-fence" the geographic area for which they are requesting data, but many don't include a map showing the area itself. Without a visual representation, there's almost no way to tell how large or small the geographic area covered by the warrant is.

Law enforcement seems to be using a three-step process to learn the names of device holders (in some cases, a single warrant authorizes all three steps). In the first step, the officer specifies the area and time period of interest, and in response, Google gives the police information on all the devices that were there, identified by anonymous numbers—this step may reveal hundreds of devices.

After that, officers can narrow the scope of their request to fewer devices, and Google will release even more detailed data, including data on where devices traveled outside the original requested area and time period. This data, which still involves multiple devices, reveals detailed travel patterns. In the final step, detectives review that travel data to see if any devices appear relevant to the crime, and they ask for the users' names and other information for specific individual devices.

This technique is problematic for several reasons. First, unlike other methods of investigation used by the police, the police don't start with an actual suspect or even a target device—they work backward from a location and time to identify a suspect. This makes it a fishing expedition—the very kind of search that the Fourth Amendment was intended to prevent. Searches like these—where the only information the police have is that a crime has occured—are much more likely to implicate innocent people who just happen to be in the wrong place at the wrong time. Every device owner in the area during the time at issue becomes a suspect—for no other reason than that they own a device that shares location information with Google.

Second, as the Supreme Court recognized in Carpenter v United States last summer, detailed travel data like this can provide "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" This is exactly what the deputy police chief recognized when he said Google location data "shows the whole pattern of life."

Third, there's a high probability the true perpetrator isn't even included in the data disclosed by Google. For these kinds of warrants, officers are just operating off a hunch that the unknown suspect had a cellphone that generated location data collected by Google. This shouldn't be enough to support probable cause, because it's just as likely that the suspect wasn't carrying an Android phone or using Google apps at the time.

Techniques like this also reveal big problems with our current warrant system. Even though the standard for getting a warrant is higher than other legal procedures—and EFF pushes for a warrant requirement for digital data and devices—warrants, alone, are no longer enough to protect our privacy. Through a single warrant the police can access exponentially more and more detailed information about us than they ever could in the past. Here, the police are using a single warrant to get access to location information for hundreds of devices. In other contexts, through a single warrant, officers can access all the data on a cell phone or a hard drive; all email stored in a Google account (possibly going back years); and all information linked to a social media account (including photos, posts, private communications, and contacts).

We shouldn’t allow the government to have such broad access to our digital lives. One way we could limit access is by passing legislation that mandates heightened standards, minimization procedures, and particularity requirements for digital searches. We already have this in laws that regulate wiretaps, where police, in addition to demonstrating probable cause, must state that they have first tried other investigative procedures (or state why other procedures wouldn’t work) and also describe how the wiretap will be limited in scope and time.

The Fourth Amendment itself also supports limits on the scope of individual warrants. It states that warrants must “particularly describ[e] the place to be searched, and the persons or things to be seized.” However, many courts merely rubber stamp warrant requests without questioning the broad scope of the request.

As the Times article notes, this technique implicates innocent people and has a real impact on people’s lives. Even if you are later able to clear your name, if you spend any time at all in police custody, this could cost you your job, your car, and your ability to get back on your feet after the arrest. One man profiled in the Times article spent nearly a week in police custody and was having trouble recovering, even months after the arrest. He was arrested at work and subsequently lost his job. Due to the arrest, his car was impounded for investigation and later repossessed. These are the kinds of far-reaching consequences that can result from overly broad searches, so courts should subject geo-location warrants to far more scrutiny.

Please follow link below for additional embedded information:

https://truthout.org/articles/googles-sensorvault-can-tell-police-where-youve-been/
