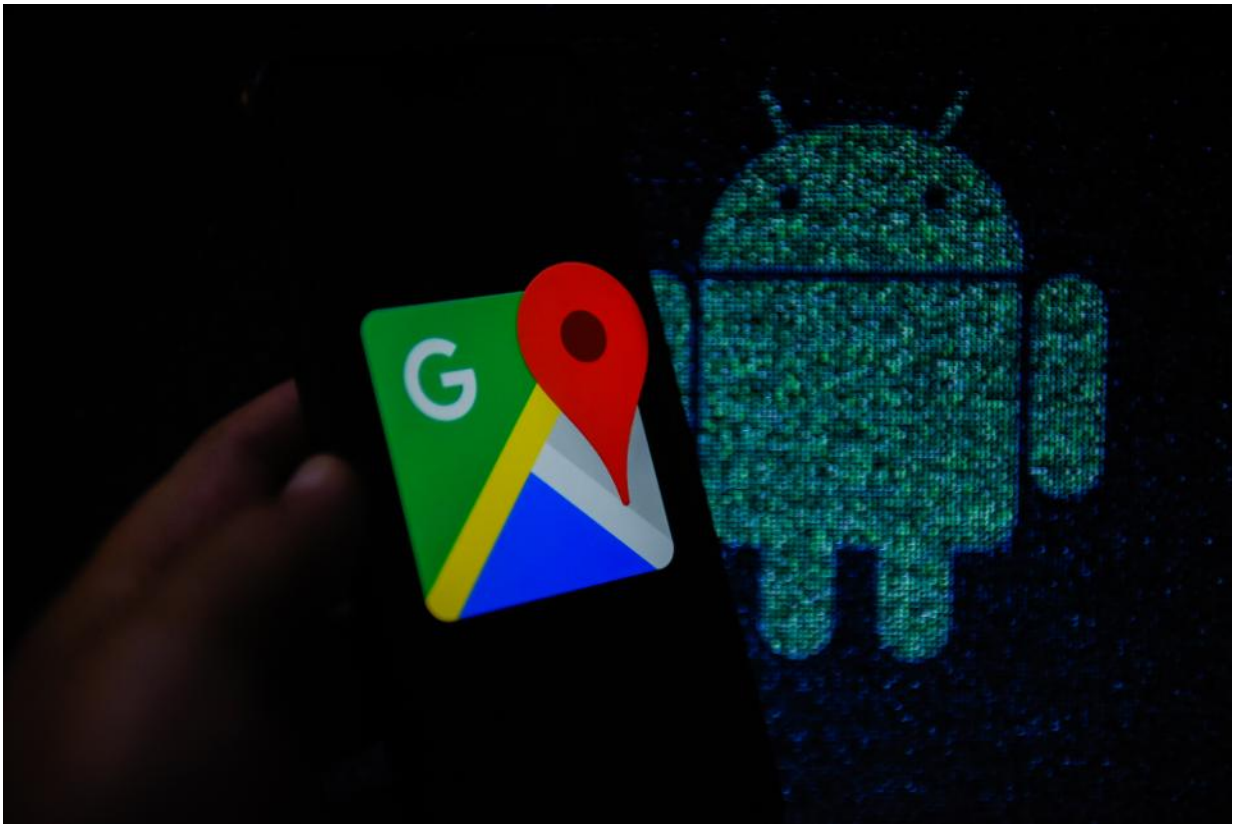
7,720 views | Aug 15, 2018, 09:00am

To Catch A Robber, The FBI Attempted An Unprecedented Grab For Google Location Data

Thomas Fox-Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.



The FBI asked Google to provide information on its users who'd been at two of nine locations at certain times, as investigators tried to find leads in an armed robbery case.

Back in March, as it investigated a spate of armed robberies across Portland, Maine, the FBI made an astonishing, unprecedented request of Google. The feds wanted the tech giant to find all users of its services who'd been within the vicinity of at least two of nine of those robberies. They limited the search to within 30-minute timeframes around when the crimes were committed. But the request covered a total space of 45 hectares and could've included anyone with an Android or iPhone using Google's tools, not just the suspect.

The FBI then demanded a lot of personal information on affected users, including their full names and addresses, as well as their Google account activity. The feds also wanted all affected users' historical locations. According to court records, while Google didn't provide the information, the cops still found their suspect in the end.

Outside of concerns around government overreach, the FBI's remarkable attempt to force Google to assist in its investigation will likely worry all who were disturbed by an *Associated Press* investigation published on Monday that claimed Google continued to track people even when they turned location features off. The court warrants unearthed by *Forbes* indicate some at the FBI believe they have a right to that location data too, even if it belongs to innocents who might be unwittingly caught up in invasive government surveillance. And the government feels such fishing expeditions are permissable; it issued the warrant on Google without knowing whether or not the suspect used an Android device or any of the company services at all.

Feds get creative

Above all, though, the documents show the FBI is getting creative in how it obtains data from Google. And it has privacy implications for all users of Google services.

Nathan Wessler, staff attorney at the American Civil Liberties Union (ACLU), told *Forbes* it was unlikely the average user of Google services would know such government searches were even possible. "I think it'd be surprising to learn that Google and other tech companies kept these kinds of records that are searchable ... to help find people at a specific location at a specific time.

"People should have an understanding of what data is being collected of theirs and how they can protect it."

Marina Medvin, an attorney and founder of Medvin Law, said the warrant amounted to "a completely indiscriminate search of a large group of people."

Despite limiting the search to users who'd been at two of the locations within certain timeframes, Medvin said the government didn't go far enough. "This is a general search, which is prohibited under our Constitution. It is not particularized, a legal prerequisite to obtain a warrant under U.S. law," she said. "The Supreme Court explained that the purpose of the particularity requirement is to make general searches impossible and to prevent 'a general, exploratory rummaging.'

"Yet, general, exploratory rummaging of a bunch of people who visited these places is exactly what would result if such a warrant were executed successfully."

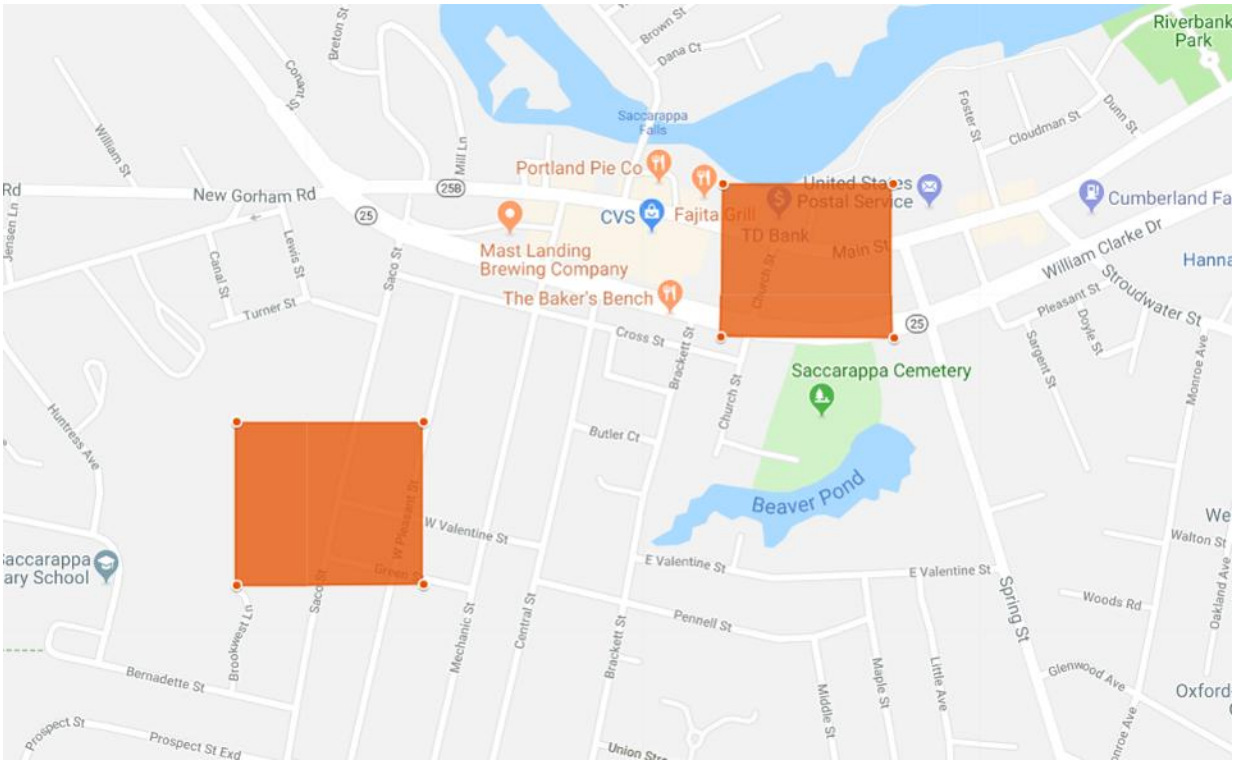
FBI gives up on Google data

It was only last week that the FBI finally gave up chasing Google for the information, having spent five months waiting.

The feds filed an initial application on March 30 for a warrant that would get them information from Android devices at nine different locations, including a Subway, two gas

stations, two Chinese restaurants, two coffee shops and two minimarts. Between March 20 and March 29, an unidentified individual (or individuals) entered those premises carrying a handgun and demanded the cashier hand over money. They stole cash totalling around $2,300.

Forbes created a Google map showing those nine separate crime scenes, covering a total of 45 hectares (approximately 110 acres) of ground. While most locations were far enough away from one another to dramatically lower the possibility of innocents being in two of the locations at the given times, two were within 500 meters of one another. They both included a significant number of residences and business premises.



Two locations where the FBI asked for Google user data were less than 500 meters apart. FORBES

In justifying the need for the warrant, FBI agent Patrick Clancy wrote it would "identify which cellular devices were near two or more of the locations where the robberies occurred at the date and time the robberies occurred, and may assist law enforcement in determining which persons were present or involved with the robberies under investigation."

Clancy didn't note whether or not personal data belonging to innocent people would be hoovered up. Nevertheless, the warrant was signed off by a judge, who also sent a so-called gag order to Google, forcing it to to keep the warrant secret from either those targeted or "any other person" for 180 days.

Google was expected to return the information on April 19, but didn't. The FBI filed a motion to extend the time it had to get the data, which a judge granted. But Google never handed it over, despite another three FBI motions to extend. Though the prosecutor, assistant U.S. attorney Michael Conley, said a fifth motion would be filed if the data didn't arrive, the government gave up the ghost earlier this month.

A final returned warrant, dated August 6, simply stated: "Google did not provide information responsive to the warrant."

It's unclear whether Google didn't want to give up the information, or if it simply couldn't retrieve the data. There were no filings objecting to the warrant and Google declined to comment.

Such government requests are known as reverse location warrants. Traditionally they've been sent to telecoms companies. But earlier this year, local media publication *WRAL*

reported numerous cases where Google had been sent similar orders in Raleigh, North Carolina.

What made the Maine data request unique was its complexity and breadth, asking Google to carry out significant work to find people who'd been in two locations, across multiple locations at specifc times, all in a single warrant. "This is not an old school investigavitve tecnique, it's a totally new and novel power," the ACLU's Wessler said.

It also appears to be the first known occasion that the FBI has issued such a reverse location warrant.

Cops get their man without Google

The feds didn't appear to need Google's data anyway. They still managed to find a suspect, 38-year-old Travis Card, who pled guilty earlier this month. Court records show investigators used a wide range of other surveillance techniques to tie Card to the crimes.

One was the use of footprints. They matched specific prints from an Under Armour sneaker found on snow across crime scenes. Miraculously, the FBI retrieved a missing Under Armour shoe on April 11. They then took DNA samples from the shoe, which matched those they had on record for Card.

Cops also obtained E-ZPass toll records for Card's work truck and historical cellphone location data, though it doesn't say from where, and the prosecutors declined to provide more information on that separate warrant. Wessler suspects a cellphone service provider handed over the data, most likely containing records of devices that hit particular cell towers.

"This general kind of request is something we've seen a lot directed at cellphone service providers in terms of tower dumps,' he added. "It can be powerful, but it's also a tool that sweeps up data on a large number of innocent people."

Card's attorney said she had no idea about the government's request for Google data until yesterday.

"I would have been all over it if Travis exercised his right to a trial. It is mind-blowing that the federal government believes this is not a blatant violation of privacy," Heather Gonzales of law firm Strike Gonzales & Butler Bailey.

"Bottom line, when an investigation violates the Constitution, the evidence can't be used at trial, which often results in dismissals of the charges, regardless of what the evidence was, which means some suspects who could have been convicted just walk right out of the courtroom. The hubris defeats the goal."

Got a tip? Get me on Signal on +447837496820 or use SecureDrop to tip anyone at Forbes. Email at TFox-Brewster@forbes.com or tbthomasbrewster@gmail.com for PGP mail.

I cover security and privacy for Forbes. I've been breaking news and writing features on these topics for major publications since 2010. As a freelancer, I worked for The Guardian, Vice Motherboard, Wired and BBC.com, amongst many others. I was named BT Security Journalist o... MORE