Google Tracks Your Location and Shares It With Police and DNC, Even When Your Phone is Off

TOPICS:ConstitutionConsumer RightsGoogleNSAPolicePrivacySensorvaultsmart technologySurveillance

By Derrick Broze

Even if you disable GPS, deactivate phone location tracking, and turn off your phone, it's still possible for Google and the NSA to monitor your every move.

Over the last two decades, cellphone use has become an everyday part of life for the vast majority of people around the planet. Nearly without question, consumers have chosen to carry these increasingly smart devices with them everywhere they go. Despite surveillance revelations from whistleblowers like Edward Snowden, the average smartphone user continues to carry the devices with little to no security or protection from privacy invasions.

Americans make up one of the largest smartphone markets in the world today, yet they rarely question how intelligence agencies or private corporations might

be using their smartphone data. A recent report from the *New York Times* adds to the growing list of reasons why Americans should be asking these questions. According to the *Times*, law enforcement have been using a secret technique to figure out the location of Android users. The technique involves gathering detailed location data collected by Google from Android phones, iPhones, and iPads that have Google Maps and other Google apps installed.

The location data is stored inside a Google database known as Sensorvault, which contains detailed location records of hundreds of millions of devices from around the world. The records reportedly contain location data going back to 2009. The data is collected whether or not users are making calls or using apps.

The Electronic Frontier Foundation (EFF) says police are using a single warrant—sometimes known as a "geo-fence" warrant—to access location data from devices that are linked to individuals who have no connection to criminal activity and have not provided any reasonable suspicion of a crime. Jennifer Lynch, EFF's Surveillance Litigation Director, says these searches are 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," Lynch wrote. "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 occurred—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."

The problems associated with Sensorvault have also concerned a bipartisan group of lawmakers who recently sent a letter to Google CEO Sundar Pichai. The letter from Democrats and Republicans on the U.S. House Energy and Commerce Committee gives Google until May 10 to provide information on how this data is used and shared. The letter was signed by Democratic Representatives Frank Pallone and Jan Schakowsky and Republicans Greg Walden and Cathy McMorris Rodgers.

Google has responded to the report from the *Times* by stating that users opt-in to collection of the location data stored in Sensorvault. A Google representative also told the lawmakers that users "can delete their location history data, or turn off the product entirely, at any time." Unfortunately, this explanation falls flat when

one considers that Android devices log location data by default and that it is notoriously difficult to opt-out of data collection.

No matter what promises Google makes, readers should remember that back in 2010, the *Washington Post* published a story focusing on the growth of surveillance by the National Security Agency. That report detailed an NSA technique that "enabled the agency to find cellphones even when they were turned off." The technique was reportedly first used in Iraq in pursuit of terrorist targets. Additionally, it was reported in 2016 that a technique known as a "roving bug" allowed FBI agents to eavesdrop on conversations that took place near cellphones.

These tools are now undoubtedly being used on Americans. The reality is that these tools—and many, many others that have been revealed—are being used to spy on innocent Americans, not only violent criminals or suspects. The only way to push back against this invasive surveillance is to stop supporting the companies responsible for the techniques and data sharing. Those who value privacy should invest time in learning how to protect data and digital devices. Privacy is quickly becoming a relic of a past era and the only way to stop it is to raise awareness, opt-out of corporations that don't respect privacy, and protect your data.

Derrick is the founder of TCRN.