Google collects Android users' locations even when location services are disabled

Covert tracking. (Reuters/Stephen Lam)

SHARE

WRITTEN BY
Keith Collins

OBSESSION
Messaging

Many people realize that smartphones track their locations. But what if you actively turn off location services, haven't used any apps, and haven't even inserted a carrier SIM card?

Even if you take all of those precautions, phones running Android software gather

November 21, 2017

data about your location and send it back to Google when they're connected to the internet, a Quartz investigation has revealed.

Since the beginning of 2017, Android phones have been collecting the addresses of nearby cellular towers—even when location services are disabled—and sending that data back to Google. The result is that Google, the unit of Alphabet behind Android, has access to data about individuals' locations and their movements that go far beyond a reasonable consumer expectation of privacy.

Quartz observed the data collection occur and contacted Google, which confirmed the practice.

The cell tower addresses have been included in information sent to the system Google uses to manage push notifications and messages on Android phones for the past 11 months, according to a Google spokesperson. They were never used or stored, the spokesperson said, and the company is now taking steps to end the practice after being contacted by Quartz. By the end of November, the company said, Android phones will no longer send cell-tower location data to Google, at least as part of this particular service, which consumers cannot disable.

"In January of this year, we began looking into using Cell ID codes as an additional signal to further improve the speed and performance of message delivery," the Google spokesperson said in an email. "However, we never incorporated Cell ID into our network sync system, so that

data was immediately discarded, and we updated it to no longer request Cell ID."

It is not clear how cell-tower addresses, transmitted as a data string that identifies a specific cell tower, could have been used to improve message delivery. But the privacy implications of the covert location-sharing practice are plain. While information about a single cell tower can only offer an approximation of where a mobile device actually is, multiple towers can be used to triangulate its location to within about a quarter-mile radius, or to a more exact pinpoint in urban areas, where cell towers are closer together.

The practice is troubling for people who'd prefer they weren't tracked, especially for those such as law-enforcement officials or victims of domestic abuse who turn off location services thinking they're fully concealing their whereabouts. Although the data sent to Google is encrypted, it could potentially be sent to a third party if the phone had been compromised with spyware or other methods of hacking. Each phone has a unique ID number, with which the location data can be associated.

The revelation comes as Google and other internet companies are under fire from lawmakers and regulators, including for the extent to which they vacuum up data about users. Such personal data, ranging from users' political views to their purchase histories to their locations, are

foundational to the business successes of companies like Facebook and Alphabet, built on targeted advertising and personalization and together valued at over $1.2 trillion by investors.

The location-sharing practice does not appear to be limited to any particular type of Android phone or tablet; Google was apparently collecting cell tower data from all modern Android devices before being contacted by Quartz. A source familiar with the matter said the cell tower addresses were being sent to Google after a change in early 2017 to the Firebase Cloud Messaging service, which is owned by Google and runs on Android phones by default.

Even devices that had been reset to factory default settings and apps, with location services disabled, were observed by Quartz sending nearby cell-tower addresses to Google. Devices with a cellular data or WiFi connection appear to send the data to Google each time they come within range of a new cell tower. When Android devices are connected to a WiFi network, they will send the tower addresses to Google even if they don't have SIM cards installed.

"It has pretty concerning implications," said Bill Budington, a software engineer who works for the Electronic Frontier Foundation, a nonprofit organization that advocates for digital privacy. "You can kind of envision any number of circumstances where that could be extremely sensitive information that puts a person at risk."

The section of Google's privacy policy that covers location sharing says the company will collect location information from devices that use its services, but does not indicate whether it will collect data from Android devices when location services are disabled:

> When you use Google services, we may collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that may, for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers.

According to the Google spokesperson, the company's system that controls its push notifications and messages is "distinctly separate from Location Services, which provide a device's location to apps." Android devices never offered consumers a way to opt out of the collection of cell tower data.

"It is really a mystery as to why this is not optional," said Matthew Hickey, a security expert and researcher at Hacker House, a security firm based in London. "It seems quite intrusive for Google to be collecting such information that is only relevant to carrier networks when there are no SIM card or enabled services."

While Google says it doesn't use the location data it collects using this service, its does allow advertisers to target consumers using location data, an approach that has obvious commercial value. The company can tell using precise location tracking, for example, whether an individual with an Android phone or running Google apps has set foot in a specific store, and use that to target the advertising a user subsequently sees.