Dear Android Users: Google Is Tracking You Even If You Disable Location Services

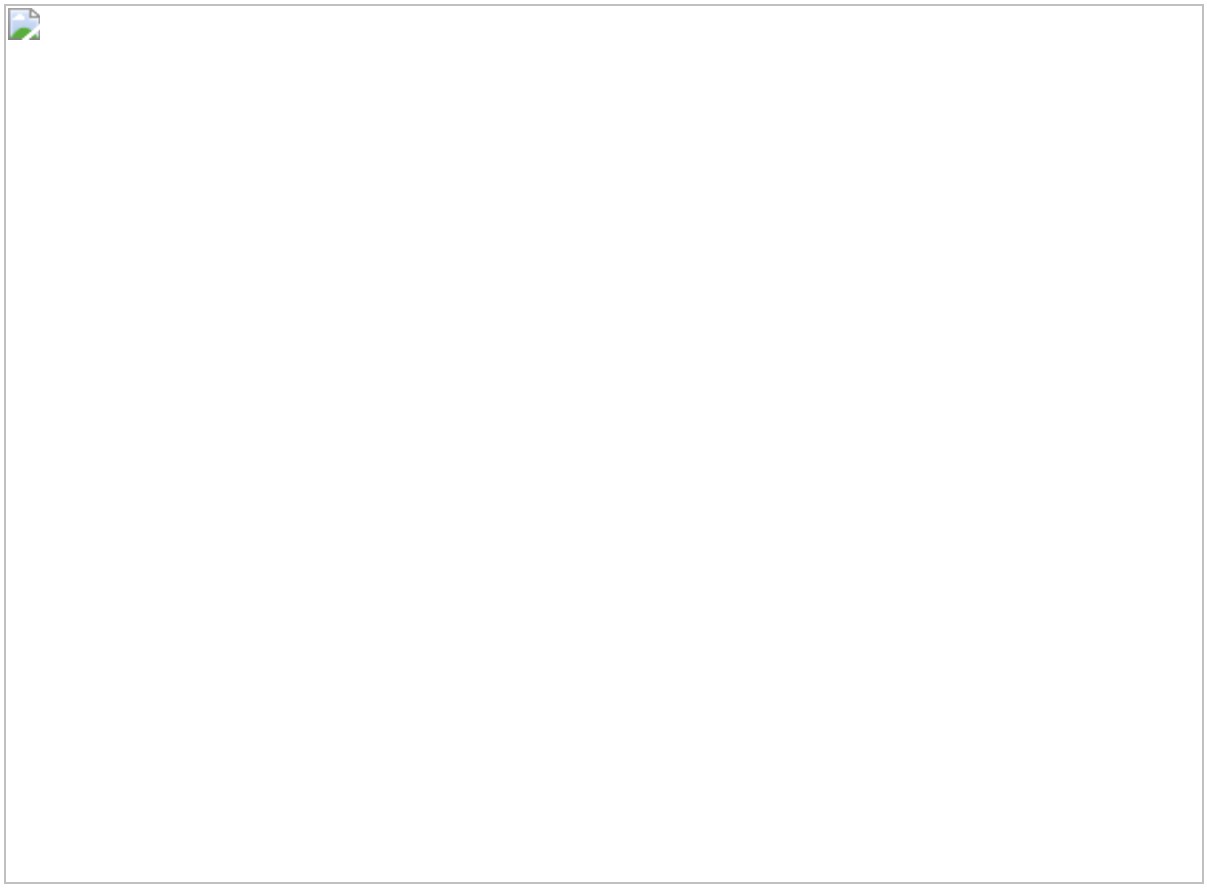
by Tyler Durden
Nov 21, 2017 7:10 PM

Slowly but surely, Americans have been conditioned to give up any expectations of privacy in the name of public safety and/or for simple technological conveniences. However, there remains, even today, a tiny sliver of the population that would prefer to not have their every movement tracked no matter how antiquated that makes them look. Be that as it may, per a recent discovery from Quartz, those old-school folks better hope they haven't been using an Android device for the past 11 months.

> 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 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.



Of course, the company that has been collecting your location data for nearly a year now without your knowledge, would like for you to know that you shouldn't worry too

much about your privacy because they can assure you the **data was never "used or stored"** and was only collected to **help "improve the speed and performance of message delivery"....**

> **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."

...you know, **because wireless carriers haven't quite figured out yet how to efficiently route data streams through network nodes just yet**...

> 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.

"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."**

"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.”**

Of course, if their excuse for this gross invasion of privacy is even remotely true, then we look forward Google's follow-up report to Android users detailing precisely how much faster their text messages are now than before...we won't hold our breath.