



Written by [Joe Wolverton, II, J.D.](#) on January 17, 2019

Cellphone Location Data for Sale on Black Market, Investigation Reveals

T-Mobile, AT&T, and Sprint sell their customers' location data to third parties, who then dispose of the data themselves, with the information ending up available to anyone willing to pay the price.

This is the remarkable story revealed in an investigation conducted by Motherboard and reported this week. Here's the background:



Nervously, I gave a bounty hunter a phone number. He had offered to geolocate a phone for me, using a shady, overlooked service intended not for the cops, but for private individuals and businesses. Armed with just the number and a few hundred dollars, he said he could find the current location of most phones in the United States.

The bounty hunter sent the number to his own contact, who would track the phone. The contact responded with a screenshot of Google Maps, containing a blue circle indicating the phone's current location, approximate to a few hundred metres [sic].

Queens, New York. More specifically, the screenshot showed a location in a particular neighborhood — just a couple of blocks from where the target was. The hunter had found the phone (the target gave their consent to Motherboard to be tracked via their T-Mobile phone.)

The bounty hunter did this all without deploying a hacking tool or having any previous knowledge of the phone's whereabouts. Instead, the tracking tool relies on real-time location data sold to bounty hunters that ultimately originated from the telcos themselves, including T-Mobile, AT&T, and Sprint ... sometimes sold through word-of-mouth networks.

That's a lot to unpack, but the upshot is this: There are private companies that buy the ability to track your GPS location from the world's premier telecommunications companies and then sell that data to individuals, without regard to whether all the parties in the stream of commerce can legally control that data.

It doesn't end there, though. The Motherboard story claims that the ability to track the locations of cellphone owners is available on the black market and is often bought and sold among entities "who are not licensed by the [telco] to use it."

Incredibly, I have personal experience with this illicit peddling of private data.

While practicing law, I knew of individuals claiming to be "private investigators" who, through word of mouth, advertised their ability to track people who skipped bail using cellphone GPS data.



Written by [Joe Wolverton, II, J.D.](#) on January 17, 2019

I neither purchased such information, nor pursued business dealings with those purporting to have access to it. I can attest, however, that such “services” were offered.

Those unfamiliar with the telcos’ tracking technology may not appreciate just how harmful such unauthorized access can be.

Your cellphone is constantly sending out signals to towers that triangulate your location. This data is stored by the company and with a few keyboard clicks, your precise location is (in some cases it is an approximation based on pings to towers) shown in real-time.

This creepy capacity is consented to by anyone purchasing a cellphone plan. Granted, it is in the small print that most of us never read, but it is culturally understood that one of the compromises we make for mobile communication is mobile location tracking.

Legally, the companies providing us with cell service are bound by federal regulations to protect that data, making it available only to licensed “location aggregators,” companies that themselves must comply with industry regulations, as well.

Problem is, those aggregators are offering the data to “a spread of different private industries, ranging from car salesmen and property managers to bail bondsmen and bounty hunters,” Motherboard reports.

On January 10, the *Washington Post* reported that AT&T “will stop selling its customers’ location data to third-party service providers” in the wake of the Motherboard exposé and threats from lawmakers on Capitol Hill to investigate the details of the story of sordid commerce.

Senator Ron Wyden (D-Ore.), a reliable defender of privacy, took to Twitter to call out the companies’ lackadaisical crackdown on the misuse of the location data they collect, collate, and sell. “Major carriers pledged to end these practices, but it appears to have been more empty promises to consumers,” Wyden tweeted.

That seemed to have lit a fire under the telecommunications titans taken to task in the Motherboard investigation. “In light of recent reports about the misuse of location services, we have decided to eliminate all location aggregation services — even those with clear consumer benefits,” AT&T said in a public statement. “We are immediately eliminating the remaining services and will be done in March.”

T-Mobile and Verizon followed suit, insisting that they would discontinue providing customers’ geolocation data to third-parties unless the customers “give the company permission to share their data with roadside assistance firms.”

Of course, one would be tempted to callously chalk up all this circulation of customer location data to the cost of carrying around a little computer in your pocket. That attitude would be attractive if not for the intimate relationship between the telcos and the federal government, and between the telcos and law enforcement.

It’s one thing for a private company to take the personal information it collects about its customers and package those up for resale if the entire marketplace was private and the customers knew such sales were likely.

That is not the situation here, though. The companies not only intentionally and perhaps unlawfully violated the agreements made with their customers, but these global corporations apparently used none of their vast resources to exercise any acceptable amount of precaution over the hands into which their customers’ GPS location fell.



Written by [Joe Wolverton, II, J.D.](#) on January 17, 2019

Regardless of how soon and how thoroughly AT&T, Sprint, Verizon, and T-Mobile terminate their practices of packaging and selling location data, ultimately the prevention of future flare-ups of these exchanges is in the hands of the customers whose data is being sold.

As renowned economist Ludwig von Mises wrote:

The real bosses, in the capitalist system of market economy, are the consumers. They, by their buying and by their abstention from buying, decide who should own the capital and run the plants. They determine what should be produced and in what quantity and quality. Their attitudes result either in profit or in loss for the enterpriser.

Photo: [Clipart.com](#)



Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



Subscribe

What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.