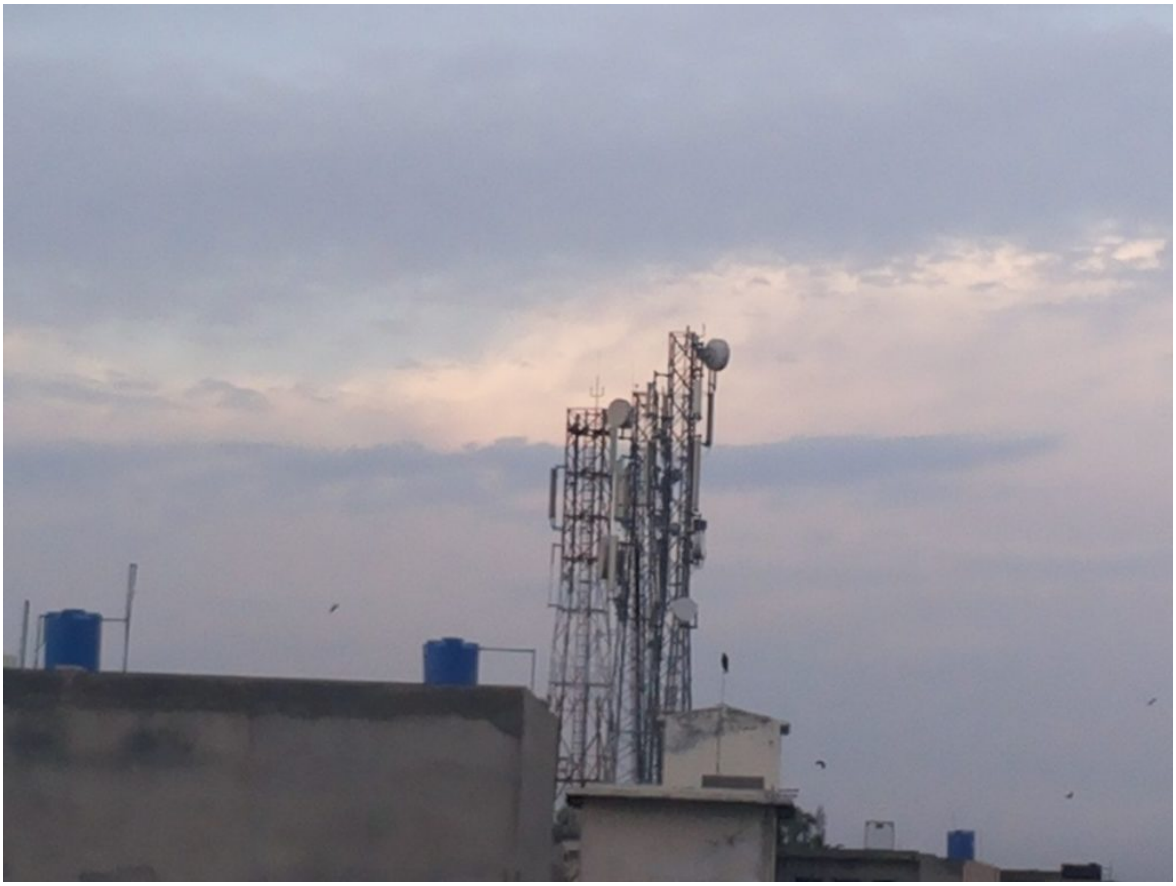

How T-Mobile, Sprint & AT&T Sell Your Smartphone Geo-Location Data

Are you happy that every Tom, Dick and Harry in the world can pinpoint your location and track your whereabouts like the CIA? Mega-carriers apparently gain huge profits by selling your location data to private, and often shady, data mining companies, who in turn sell it to others. This makes mockery of every privacy agreement ever offered by these companies. TN Editor

T-Mobile, Sprint, and AT&T are selling access to their customers' location data, and that data is ending up in the hands of bounty hunters and others not authorized to possess it, letting them track most phones in the country.

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.

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, a Motherboard investigation has found. These surveillance capabilities are sometimes sold through word-of-mouth networks.

Whereas it's common knowledge that law enforcement agencies can track phones with a warrant to service providers, IMSI catchers, or until recently via other companies that sell location data such as one called Securus, at least one company, called Microbilt, is selling phone geolocation services with little oversight to a spread of different private industries, ranging from car salesmen and property managers to bail bondsmen and bounty hunters, according to sources familiar with the company's products and company documents obtained by Motherboard. Compounding that already highly questionable business practice, this spying capability is also being resold to others on the black market who are not licensed by the company to use it, including me, seemingly without Microbilt's knowledge.

Motherboard's investigation shows just how exposed mobile networks and the data they generate are, leaving them open to surveillance by ordinary citizens, stalkers, and criminals, and comes as media and policy

makers are paying more attention than ever to how location and other sensitive data is collected and sold. The investigation also shows that a wide variety of companies can access cell phone location data, and that the information trickles down from cell phone providers to a wide array of smaller players, who don't necessarily have the correct safeguards in place to protect that data.

"People are reselling to the wrong people," the bail industry source who flagged the company to Motherboard said. Motherboard granted the source and others in this story anonymity to talk more candidly about a controversial surveillance capability.

Your mobile phone is constantly communicating with nearby cell phone towers, so your telecom provider knows where to route calls and texts. From this, telecom companies also work out the phone's approximate location based on its proximity to those towers.

Although many users may be unaware of the practice, telecom companies in the United States sell access to their customers' location data to other companies, called location aggregators, who then sell it to specific clients and industries. Last year, one location aggregator called LocationSmart faced harsh criticism for selling data that ultimately ended up in the hands of Securus, a company which provided phone tracking to low level enforcement without requiring a warrant. LocationSmart also exposed the very data it was selling through a buggy website panel, meaning anyone could geolocate nearly any phone in the United States at a click of a mouse.

There's a complex supply chain that shares some of American cell phone users' most sensitive data, with the telcos potentially being unaware of how the data is being used by the eventual end user, or even whose hands it lands in. Financial companies use phone location data to detect fraud; roadside assistance firms use it to locate stuck customers. But AT&T, for example, told Motherboard the use of its customers' data by bounty hunters goes explicitly against the company's policies, raising questions about how AT&T allowed the sale for this purpose in the first place.

“The allegation here would violate our contract and Privacy Policy,” an AT&T spokesperson told Motherboard in an email.

In the case of the phone we tracked, six different entities had potential access to the phone’s data. T-Mobile shares location data with an aggregator called Zumigo, which shares information with Microbilt. Microbilt shared that data with a customer using its mobile phone tracking product. The bounty hunter then shared this information with a bail industry source, who shared it with Motherboard.

Read full story here…