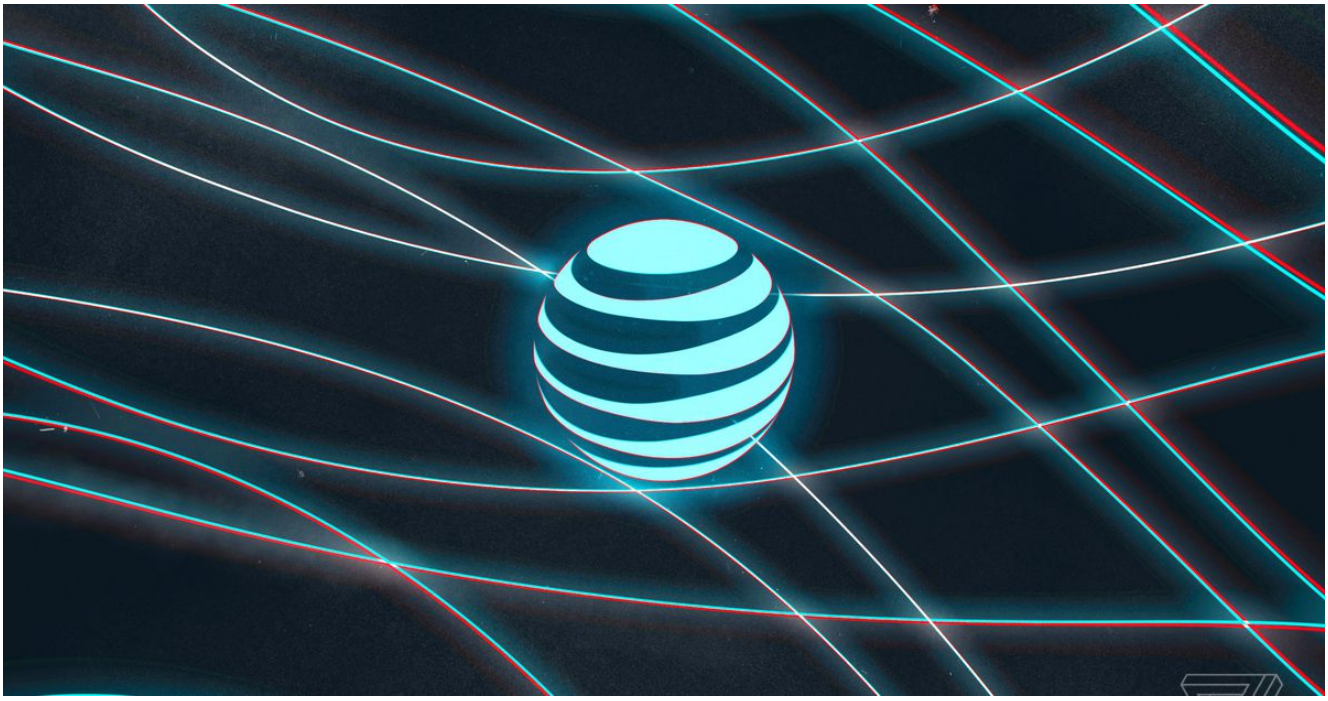
AT&T defends location data sales in newly public letter



AT&T defended the sale of user location data in a letter made public today, saying that the practice was technically legal because it did not involve the type of data the Federal Communications Commission prohibits carriers from selling without user consent. Despite that defense, the company claims it has, in the past few months, accelerated its plan to stop providing such data, which, again, AT&T would very much like to remind everyone wasn't against the law.

The FCC is investigating the telecom and fellow carriers T-Mobile, Sprint, and Verizon for the long-standing practice that only in the past couple of years has come to light after press investigations. All four major carriers claimed they would stop the practice in June 2018 after a security breach exposed sensitive user data, but new revelations about location information acquired by bounty hunters on the black market have undermined the companies' pledges.

AT&T says the type of GPS data it provided to aggregators didn't violate federal law

Verizon was the first company to say it would stop providing such data to aggregators and would only give it to roadside assistance providers. The other carriers followed with similar provisions for law enforcement and emergency requests. However, earlier this year, it was discovered that the data was still being made available to some third-party companies like Zumigo and Microbilt, which were easily accessible by bounty hunters, *Motherboard* found. The carriers claimed the fault lies with its partners for not handling the data appropriately and deleting it when necessary, and lawmakers have applied increased pressure on the companies to follow through on the promise to take action and end the agreements.

According to AT&T's letter, the type of data it has provided to third parties without user consent is not in violation of federal law, specifically its use of data known as A-GPS. The company is basing this is on a bit of a technicality, saying A-GPS data, which is gathered the company claims for use both by emergency services and for GPS-based services like ride-hailing apps, is not under the same umbrella as the data the FCC prohibits carriers from selling or data stored in what's known as the National Emergency Address Database (NEAD). AT&T says NEAD data can is more granular and can use Wi-Fi and Bluetooth data to pinpoint in-door location, whereas A-GPS is more general.

"While A-GPS is certainly used by 911 dispatchers to assist in locating individuals in emergency situations, it is also an important feature commonly used by app developers to provide location services. For example, ride-sharing apps use A-GPS to make sure the car shows up in the right location. For these reasons, reports of purported improper use of A-GPS are incorrect," AT&T writes Joan Marsh, AT&T's executive vice president of regulatory and state external affairs.

Nonetheless, AT&T said it stopped sharing location data to third-party services and aggregators in late March. "Our contracts require all parties who have received AT&T customer

location data in connection with those arrangements to delete that information and we are verifying that they have done so, subject to any of their preservation obligations," Marsh concludes. The decision to wind down its sale of such data is likely because, although AT&T may be technically correct in its interpretation of FCC rules, its sale of the data may still violate Section 222 of the Communications Act, as noted by *Ars Technica.* AT&T did not immediately respond to a request for comment.

"It is chilling to think what a black market for this data could mean in the hands of criminals, stalkers, and those who wish to do us harm."

AT&T's defense is coming to light today because the FCC is struggling internally to make headway on the investigation. "The FCC has been totally silent about press reports that for a few hundred dollars shady middlemen can sell your location within a few hundred meters based on your wireless phone data. That's unacceptable," writes Commissioner Jessica Rosenworcel, a Democrat, who has accused the Republican-controlled FCC of withholding vital information about the progress of the agency's investigation.

"I don't recall consenting to this surveillance when I signed up for wireless service – and I bet neither do you. This is an issue that affects the privacy and security of every American with a wireless phone," Rosenworcel added. "It is chilling to think what a black market for this data could mean in the hands of criminals, stalkers, and those who wish to do us harm. I will continue to press this agency to make public what it knows about what happened. But I do not believe consumers should be kept in the dark. That is why I am making these letters available today."

T-Mobile, Sprint, and Verizon were less defensive in letters also published by Rosenworcel today. Verizon says it halted all sales of such data to third parties back in November 2018, and it ended its deals with roadside assistance companies in

March. T-Mobile says it took a similar action, notifying its providers last fall that it would be ending its contracts with location-based service providers and doing so in March.

Sprint, on the other hand, says it's in the process of ending its contracts. "In response to your questions. Sprint is currently only using one location aggregator to provide [location-based services] to two customers with a public interest – a provider of roadside assistance for Sprint customers, and a provider that facilitates compliance with state requirements for a lottery that funds state government," Sprint privacy chief Maureen Cooney wrote. "As of May 31, 2019, Sprint will no longer contract with any location aggregators to provide LBS. Sprint anticipates that after May 31. 2019, it may provide LBS services directly to customers like those described above, but there are no firm plans at this time."

https://www.theverge.com/2019/5/17/18629553/att-t-mobile-sprint-verizon-selling-user-location-data-illegal-fcc-letters-public