FRANK PALLONE, JR., NEW JERSEY
CHAIRMAN

GREG WALDEN, OREGON
RANKING MEMBER

ONE HUNDRED SIXTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

January 16, 2019

Mr. Randall Stephenson
Chairman and Chief Executive Officer
AT&T
208 South Akard Street
Dallas, TX 75202

Dear Mr. Stephenson:

We write with questions regarding the privacy policies and guidelines regarding location-based information and services that AT&T and the wireless telecommunications industry have in place. According to a recent *Motherboard* investigative report, nationwide wireless carriers may be continuing to sell American customers' real-time location data and information to various third parties without customers' knowledge and consent.[1] According to the report, Zumigo, a location aggregation firm, purchased geolocation data from T-Mobile, and subsequently sold that data to Microbilt, a third party firm, which further disseminated the geolocation data to another company and intermediary. This practice of selling and sharing of location information through multiple entities potentially impacts hundreds of millions of American customers. We are deeply troubled because it is not the first time we have received reports and information about the sharing of mobile users' location information involving a number of parties who may have misused personally identifiable information.

In July 2018, we wrote to LocationSmart, Securus Technologies, and 3CInteractive regarding location sharing practices.[2] At that time, media reports alleged that Securus, a prison communications firm, impermissibly allowed U.S. law enforcement to request location information through LocationSmart, and potentially 3C as an intermediary between the parties, for investigative or surveillance purposes.[3] LocationSmart was then one of two commercial

---

[1] Joseph Cox, "I Gave a Bounty Hunter $300. Then He Located Our Phone," Motherboard, January 8, 2019, at https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

[2] https://republicans-energycommerce.house.gov/news/letter/letters-to-locationsmart-securus-technologies-and-3cinteractive-regarding-location-sharing-practices/

[3] Jennifer Valentino-DeVries, "Service Meant to Monitor Inmates' Calls Could Track You, Too," *New York Times*, May 10, 2018, at https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html

businesses (including Zumigo) that T-Mobile had engaged as part of the company's location aggregator program.[4] Location aggregator firms manage and process requests for location information from AT&T as well as Sprint, T-Mobile and Verizon on behalf of their corporate customers who provide authorized, downstream commercial services. AT&T acknowledged in 2018 that it had a privacy policy, or location aggregator program guidelines, in place providing for authorized use of location data by location aggregators in certain situations.[5] However, if the 2018 allegations were true, providing location information to correctional officers at prison facilities would have violated some or all of AT&T's policies relating to use of real-time geolocation data.

The recent *Motherboard* report alleged that a reporter purchased the real-time location of a mobile phone from a bail industry source for $300.[6] The bail industry source engaged a bail bond company which, in turn, used third-level firm Microbilt to confirm the location of the phone. The report states that the "Google Maps screenshot provided to Motherboard of the target phone's location also included its approximate longitude and latitude coordinates, and a range of how accurate the phone geolocation is: 0.3 miles, or just under 500 metres."[7]

In this instance, the real-time location data access appears to have begun with T-Mobile, before moving to the location aggregator company Zumigo, then to Microbilt, and then to subsequent sources. At no point does it appear that the target phone received an explicit notice that it was being tracked.

Last year, we were similarly troubled by reports that third parties may not have provided clear notice to customers and obtained affirmative opt-in consent from those customers before they provided personally identifiable customer location information. In both instances, if third parties did not obtain affirmative consent directly from wireless customers, then no location aggregator nor any U.S. wireless carrier should have been able to grant location information access. Similarly, if location aggregators, such as Zumigo and LocationSmart, and other intermediaries, including Microbilt, Securus, and customers that use their platforms like bail bond companies, in the supply chain were relying on delegated consent by the next actor in the chain then there should be a record of consent by each party. In either case, however, it appears there may have been a failure in obtaining direct or delegated consent from the customer.

Subsequent to last year's media reports about location information concerns, AT&T wrote:

> "After learning about the Securus On-Demand Service, AT&T took prompt steps to protect customer data and shut down 3Cinteractive and Securus's access to the AT&T customer location data. On May 10, 2018, within two days of receiving your letter,

---

[4] Letter from Anthony Russo, Vice President-T-Mobile US, Inc., to Senator Ron Wyden, dated June 15, 2018.
[5] Letter from Timothy P. McKone, Executive Vice President-Federal Relations, AT&T, to Senator Ron Wyden, dated June 15, 2018
[6] Joseph Cox, "I Gave a Bounty Hunter $300. Then He Located Our Phone," Motherboard, January 8, 2019, at https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile
[7] Id.

> AT&T terminated Securus's access to customer information in connection with the On-Demand Service. And on May 16, 2018, after learning that Securus may have suffered a data breach that compromised the log-in credentials of its corrections and law enforcement customers, AT&T suspended the provision of all customer location information to Securus for any purposes, including the Inmate Calling Service.
>
> AT&T has no reason to believe that there are other instances of unauthorized access to AT&T customer location data. Nonetheless, we are reviewing these issues carefully to ensure the proper handling of all AT&T customer information."[8]

The January 2019 *Motherboard* report raises fresh, serious questions about how U.S. wireless carriers and third parties are accessing, transferring, storing, and securing customer location information. Accordingly, we request AT&T's assistance to better understand the various issues relating to location information and their impact on consumers, and ask that you respond to the following questions no later than January 30, 2019:

1. Does AT&T have any current contracts in force with Zumigo? Is Zumigo still able to access location information from AT&T? If not, what were the closing dates for the contracts and/or the information sharing?

2. Does AT&T have any current contracts in force with LocationSmart, 3CInteractive or Securus Technologies? Are LocationSmart, 3CInteractive or Securus Technologies still able to access location information from AT&T? If not, what were the closing dates for the contracts and/or the information sharing?

3. Please identify any additional third parties which AT&T has shared location data and information with at any time since 2007.

4. Please provide a list of location-information elements and records that AT&T provides location aggregators.

5. Please provide a list of location-information elements and records that AT&T's location aggregator partners are authorized to provide to each of its corporate customers.

6. If a location aggregator, like Zumigo or LocationSmart, does not gain consent from a mobile phone owner or user, can it disclose the location information provided by AT&T? If relies on delegated consent, secured by its corporate client or another third party, how does AT&T verify and record the other third parties have secured consent?

7. What are the terms of service, or contractual arrangements, between AT&T and Zumigo, or AT&T and any other participant in the location data service? What steps has AT&T taken, or can take, for any violations of its terms of services?

---

[8] Letter from Timothy P. McKone, Executive Vice President-Federal Relations, AT&T, to Senator Ron Wyden, dated June 15, 2018.

8. How many third parties have AT&T's authorized location aggregators contracted with to provide location information services?

9. What are the terms of service, or contractual arrangements, between AT&T and third parties selling and sharing real-time location data and information? What steps has AT&T taken, or can take, for any violations of its terms of services?

10. How does AT&T ensure that location aggregators or third parties are selling services and products that are specific and approved under its terms of service?

11. How does AT&T evaluate the efficacy of its independent third party audit program to ensure a location aggregator's corporate customers are obtaining requisite customer consent prior to using location information and in compliance with the company's supplier integrity standards?

12. Please provide a list of which third party auditors provided compliance services related to the location data service. Will AT&T make those audit reports available for Committee review?

13. What are AT&T's preliminary conclusions of any internal or independent audits conducted in connection with the LocationSmart and Zumigo disclosures described above?

14. What is AT&T's process for screening and authorizing third party access to location information, including evaluating and auditing whether a location aggregator or third party is engaged in AT&T's pre-approved, authorized activities contemplated for location aggregators and intermediaries?

15. Is AT&T aware of any other incidents of inappropriate or unlawful use of location information through a location aggregator or another third party since 2007?

Please also make arrangements to provide Committee staff with a briefing on these topics by January 30, 2019. If you have any questions, please contact Melissa Froelich, Robin Colwell, and Jennifer Barblan of the Committee staff at (202) 225-2927. Thank you for your prompt attention to this request.

Sincerely,

Greg Walden
Republican Leader
Committee on Energy and Commerce

Cathy McMorris Rodgers
Republican Leader
Subcommittee on Consumer Protection
and Commerce

Robert E. Latta
Republican Leader
Subcommittee on Communications
and Technology

Brett Guthrie
Republican Leader
Subcommittee on Oversight
and Investigations