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. Hans Vestberg
Chief Executive Officer
Verizon
1095 Avenue of the Americas
New York, NY 10013

Dear Mr. Vestberg:

We write with questions regarding the privacy policies and guidelines regarding location-based information and services that Verizon 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 Verizon as well as AT&T, Sprint and T-Mobile on behalf of their corporate customers who provide authorized, downstream commercial services. Verizon 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 Verizon'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, Verizon wrote:

> "We have decided to end our current location aggregation arrangements with LocationSmart and Zumigo. Verizon has notified these location aggregators that it intends to terminate their ability to access and use our customers' location data as soon as possible. This termination, however, must be completed in careful steps so as not to

---

[4] Letter from Anthony Russo, Vice President-T-Mobile US, Inc., to Senator Ron Wyden, dated June 15, 2018.
[5] Letter from Karen Zacharia, Chief Privacy Officer, Verizon, 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.

> disrupt beneficial services being provided using customer location data, such as the fraud prevention and call routing services described above. Verizon will work with the aggregators to ensure a smooth transition for these beneficial services to alternative arrangements so as to minimize the harm caused to customers and end users. In the interim, Verizon will not authorize any new uses of location information by either LocationSmart or Zumigo or the sharing of location information with any new customers of these existing aggregators.."[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 Verizon'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 Verizon have any current contracts in force with Zumigo? Is Zumigo still able to access location information from Verizon? If not, what were the closing dates for the contracts and/or the information sharing?

2. Does Verizon 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 Verizon? If not, what were the closing dates for the contracts and/or the information sharing?

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

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

5. Please provide a list of location-information elements and records that Verizon'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 Verizon? If relies on delegated consent, secured by its corporate client or another third party, how does Verizon verify and record the other third parties have secured consent?

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

8. How many third parties have Verizon's authorized location aggregators contracted with to provide location information services?

---

[8] Letter from Karen Zacharia, Chief Privacy Officer, Verizon, to Senator Ron Wyden, dated June 15, 2018.

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

10. How does Verizon 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 Verizon 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 Verizon make those audit reports available for Committee review?

13. What are Verizon's preliminary conclusions of any internal or independent audits conducted in connection with the LocationSmart and Zumigo disclosures described above?

14. What is Verizon'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 Verizon's pre-approved, authorized activities contemplated for location aggregators and intermediaries?

15. Is Verizon 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