

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. Walter Wojciechowski
Chief Executive Officer
Microbilt Corporation
1640 Airport Road
Suite 115
Kennesaw, Georgia 30144

Dear Mr. Wojciechowski:

We write with questions regarding the privacy policies and guidelines regarding location-based information and services that Microbilt 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,

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/>

for investigative or surveillance purposes.³ LocationSmart was then one of two commercial 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 T-Mobile as well as AT&T, Sprint and Verizon on behalf of their corporate customers who provide authorized, downstream commercial services. T-Mobile 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 T-Mobile'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.

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 Microbilt's assistance to better understand the

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>

⁴ Letter from Anthony Russo, Vice President-Federal Legislative Affairs, T-Mobile US, Inc., to Senator Ron Wyden, dated June 15, 2018.

⁵ *Id.*

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.*

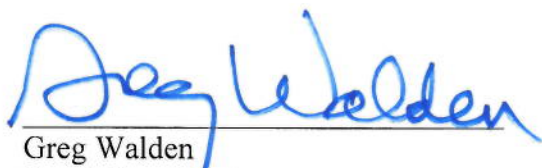
various issues relating to location information and their impact on consumers, and ask that you respond to the following questions no later than January 30, 2019:

1. What specific Microbilt services, solutions and platforms utilize location information (either coarse or precise information) provided by the wireless providers AT&T, Sprint, T-Mobile and Verizon or location aggregators like LocationSmart and Zumigo?
2. Do any of Microbilt's services, solutions, or platforms collect, aggregate, or utilize location data collected by a device—independent of wireless carrier location information—through other means; including GPS, Wi-Fi, Bluetooth, or any other means of identifying location information?
 - a. If yes, by which means does Microbilt collect, aggregate, or utilize location data?
 - b. If yes, does Microbilt rely on GPS, Wi-Fi, Bluetooth, or any other means of identifying location information to acquire precise location information?
 - i. Can Microbilt acquire precise location information solely from information collected by the wireless carrier, or are other information inputs from the device required in order to obtain precise location information?
3. Does Microbilt have any current contracts in force with Zumigo or any other location aggregator, or any U.S. wireless providers? Is the company still able to access any location information from any wireless providers, location aggregators or other third parties?
4. Does Microbilt have any current contracts in force with any other commercial clients to provide location information-based services or technology, and is Microbilt providing access to location information to any of those commercial clients?
5. Please explain how Microbilt acquires and records opt-in consent from a mobile device owner, wireless subscriber, or user before facilitating the disclosure of location information. If Microbilt does not gain consent from an owner or user, can it disclose the location information provided by the wireless provider? If Microbilt relies on delegated consent, secured by its corporate client or another third party, how does Microbilt verify and record the other third parties have secured consent?
6. Please explain what are the terms of service, or contractual arrangements, between Microbilt and Zumigo. What steps has Zumigo taken for any violations of its terms of services?
7. Can an individual user of a location service opt-out from one of Microbilt's corporate clients or another third party? If so, how?

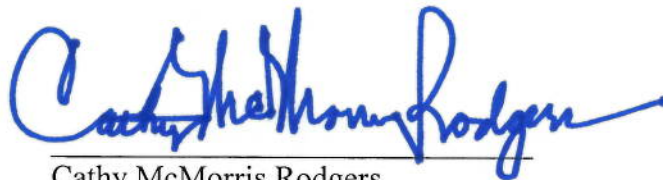
8. Please identify any additional third parties which Microbilt has shared location data and information at any time since 2007.
9. Please provide a list of location information elements and records that Microbilt is/has received from location aggregator Zumigo.
10. Please provide a list of location information elements and records that Microbilt is/was authorized by Zumigo to provide to each of Microbilt's corporate customers.
11. How does Microbilt ensure that third parties are selling services and products that are specific and approved under its terms of service?
12. Please explain whether Microbilt was/is aware of any incidents of inappropriate or unlawful use of location information through a third party?

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