601 Pennsylvania Ave., NW
North Building, Suite 800
Washington, DC 20004

February 15, 2019

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

Re: Response to Letter Dated January 17, 2019

Dear Senator Wyden,

This responds to your January 17, 2019, letter to John Legere regarding the location aggregator program in which the four national carriers participate. As explained below, as of February 8, 2019, T-Mobile has terminated all service provider access to location data under the program, and T-Mobile's LBS contracts with the Location Aggregators will officially sunset on March 9.

T-Mobile has appreciated our prior opportunities—including our meeting with your staff on September 4, 2018—to engage with you and your team and to discuss the steps T-Mobile has taken to protect its customers' location information and to prevent the misuse of that information in connection with the program. We welcome this additional opportunity to update you on the efforts we have since undertaken, and to supplement the responses in our last letter to you, dated June 15, 2018.

As we have previously explained, the program enabled T-Mobile's customers to utilize beneficial location-based services such as roadside assistance and medical emergency alerts. This program was relatively small and was similar to programs offered by other national wireless carriers. It allowed T-Mobile customers, including those without smartphones, or who did not wish to use GPS-based applications, to access location-based services. It is important to emphasize that T-Mobile's Location Aggregators and downstream location-based services ("LBS") providers did not receive location information of T-Mobile customers in bulk or under contract terms that allowed access at their discretion. Rather, they had access to location information only for specific uses approved by T-Mobile, and only upon an individual request related to that specific use and a specific customer. Each individual request for location data was required to be subject to the consent of the customer whose device was to be located.

LBS providers received T-Mobile customer location data through their contractual arrangements with our Location Aggregators, either LocationSmart or Zumigo. T-Mobile maintained strict control over our Location Aggregators through several important contractual conditions that the Location Aggregators were, in turn, contractually required to impose upon each LBS provider. Importantly, these provisions required express prior authorization of each end-user and prior T-Mobile approval for each location-based service to be offered by an LBS provider (referred to as a "use case" or "campaign"). In the rare instances when we learned of an

601 Pennsylvania Ave., NW
North Building, Suite 800
Washington, DC 20004

entity misusing customer location information, as in the cases of Securus and Microbilt, we took decisive action. Nevertheless, in light of the Securus incident, last year we undertook an evaluation of whether to retain or restructure the location aggregator program and we ultimately decided to terminate it. We notified LocationSmart and Zumigo on October 26, 2018, that we were terminating our contracts.[1] T-Mobile adopted a phased approach because we did not want to immediately terminate LBS use cases that provide important consumer benefits such as emergency assistance services without giving customers the opportunity to find alternatives. As we noted above, as of February 8, 2019, we have terminated all service provider access to location data under the program, and T-Mobile's LBS contracts with the Location Aggregators will officially sunset on March 9.

Below, T-Mobile responds to the specific questions posed in your January 17 letter.

1. Please identify the third parties with which your company shares or has shared customer information, including location data, at any time during the past five years. For each third party with which you share information directly, please also include a list of the ultimate end users of that information, as well as all intermediaries.

Response: As we noted in our June 15, 2018 response, over the past five years, T-Mobile had partnered with two location aggregators, LocationSmart (including LocAid, an aggregator acquired by LocationSmart) and Zumigo. These aggregators then partnered with LBS providers who had a direct relationship with the consumers and offered them specific location-based services with their consent. The identity of these LBS providers is proprietary and confidential business information.

The LBS providers offered various services that our customers found valuable, such as: emergency roadside assistance; emergency medical assistance; workforce/employee management/fleet tracking; charitable giving; store locator; concierge, travel and other personal services; proximity marketing; cross-carrier location aggregation; product delivery services; and mobile gaming. As mentioned below, all services were required to be provided only with the consent of the customer and after T-Mobile had approved the service and the service provider.

2. For each of the third parties identified in response to question one, please detail the types of customer information provided to them and the number of customers whose information was shared. For each of these, please detail whether the third party provided

[1] T-Mobile has a separate unrelated contract with Zumigo that will remain in place. Under that contract, which is intended to help protect T-Mobile customers from fraudulent activity, Zumigo does not have access to location information.

T-Mobile

601 Pennsylvania Ave., NW
North Building, Suite 800
Washington, DC 20004

proof of customer consent, and if so, how the third party demonstrated that they had obtained customer consent.

Response: T-Mobile's location aggregator program allowed Location Aggregators to access and transmit to the LBS provider mobile device location information for specific end users in connection with specific LBS provider campaigns that had been authorized by T-Mobile, subject to customer consent. The LBS provider had to obtain end user consent for the disclosure of location data and must have documented that consent.

3. Please describe in full your process, if any, for determining that each third party identified in response to question one has obtained appropriate customer consent before your company shared that customer's information with them. Specifically, please describe what criteria and processes your company uses to review claims and evidence that a third party has obtained consent.

Response: Both location aggregators were required to ensure verifiable informed customer consent was obtained before accessing and disclosing any network location information. In some cases, the consent was provided by the consumer to his or her service provider (*e.g.*, the roadside assistance provider). In other cases, the consent was provided from the consumer directly to the aggregator.

As noted above, T-Mobile's Location Aggregator contracts required, among other things, T-Mobile's pre-approval of the consent methods before the aggregator was permitted to access T-Mobile's customer location information. These provisions were, in turn, contractually required to be imposed by the Location Aggregator upon each LBS provider in the chain of custody of the location data. These terms included: (a) authorizing use of T-Mobile customer location data only upon the express prior authorization of the end user; (b) maintaining, and providing for T-Mobile's review, records demonstrating such consent; (c) securing T-Mobile's prior approval for each service provider and individual use; (d) appropriately securing the location data; and (e) compliance with CTIA's Guidelines for Location-Based Services.

T-Mobile required Location Aggregators to submit any new service for review and approval by T-Mobile before disclosing any customer location information in connection with that use case. The Location Aggregator was required to submit on behalf of the LBS provider a questionnaire that collected information about the service provider, its officers, its business, the service being proposed, and detailed information and documentation of the customer notice and consent processes.

The LBS provider was also required to provide T-Mobile with a clear, visual depiction of the LBS provider's proposed consent capture process. While T-Mobile did not dictate the form, placement, wording, or manner of obtaining consent, it did require that consent be informed and based on meaningful notice. To that end, T-Mobile evaluated the consent process proposed by the service provider to ensure that the customer would have clear notice regarding (1) what

location information would be provided and whether it would be shared with third parties so that users could understand what risks may be associated with such disclosures, (2) how users may withdraw consent for the disclosure of their location information, and the implications of doing so, and (3) any privacy options or controls available to users to restrict use or disclosure of location information by or to others.

Customer consent was typically obtained through one of several means: through an interactive voice response ("IVR") system in which the user is prompted to signal consent either by saying "yes" or by pressing a specific number; through an SMS message asking the user to confirm consent by message; or through a website that allows the user to manage affirmatively who can receive or use location information. In addition, in certain circumstances, consent may be obtained implicitly such as when a user requests a service that self-evidently relies on the location of the user's device, *e.g.*, when a customer signs up for roadside assistance and calls for help, the LBS provider necessarily needs the customer's location information in order to find them.

LBS providers were subject to monitoring, by the aggregator partners, to ensure compliance with these consent requirements. In turn, each aggregator was subject to periodic reviews by T-Mobile that included a sample of campaigns to ensure consents were appropriately being collected.

4. Please describe any incidents known to your company, or uncovered during your responses to the above, in which a third party with which your company shared customer data misrepresented that they had customer consent.

Response: T-Mobile is aware of five instances of alleged misuse of T-Mobile customer location information under the location aggregator program. It is important to emphasize that in all but one of these instances, the LBS provider was using T-Mobile customer location data in a manner that T-Mobile had not reviewed or approved as required under the LBS provider's respective agreements with the Location Aggregators. In each case, T-Mobile and/or the Location Aggregator took forceful steps to remedy the situation, including permanently disabling (or suspending until corrective action was taken) any transmission of T-Mobile customer location data to the LBS provider.

- On January 3, 2019, T-Mobile learned through a third party that an employee of a bail bonding company may have used a service offered by an LBS provider, Microbilt, to obtain and sell a consumer's mobile device's location information, outside the scope of the approved use case without customer consent. We understand from Microbilt that this misuse of customer location information was by a rogue employee at the bail bonding company.

- In May 2018, T-Mobile learned through a third party that an LBS provider, Securus, was offering to correctional institutions and law enforcement investigators a service that would

601 Pennsylvania Ave., NW
North Building, Suite 800
Washington, DC 20004

identify the location of a suspect's wireless device, potentially without customer consent, ostensibly on the basis of law enforcement providing a valid warrant or other legal process.

- T-Mobile learned through a third party that, in 2017, an LBS provider, LocateUrCell, was using an obfuscated website domain "cercareone.com" to provide wireless device tracking services to bail bond and similar companies without customer consent.

- In August 2014, LocAid (an aggregator since acquired by LocationSmart) informed us it was temporarily suspending an LBS provider (Freedom Telecare) due to an identified vulnerability in the consent mechanism. That vulnerability was addressed and the service was then re-enabled. There was suspicion that a bad actor, who was a paying customer of Freedom Telecare, had acquired location information without customer consent, but review of the evidence could not confirm improper disclosure of location data.

- T-Mobile also has information indicating that, in 2011, T-Mobile learned that an employee of a bail bonding company may have misused a service offered by an LBS provider, Captira, to obtain and sell a consumer's mobile device's location information without customer consent.

Sincerely,

Tony Russo

Anthony Russo
Vice President, Federal Legislative Affairs
T-Mobile US, Inc.