Joan Marsh
Chief Regulatory & State External Affairs Officer

AT&T Services, Inc.
1120 20th Street NW
Suite 1000
Washington, DC 20036

T 202.457.3120
C 202.262.7479
Jm3489@att.com

May 15, 2019

Via Email

The Honorable Jessica Rosenworcel
Commissioner
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554
Jessica.Rosenworcel@fcc.gov

Dear Commissioner Rosenworcel:

I am responding to your May 1, 2019 letter to AT&T Communications, LLC ("AT&T") CEO John Donovan, requesting information regarding AT&T's provision of location-based services. The protection of our customers' privacy is a top priority at AT&T.

As you are aware, in June 2018, AT&T announced it would be phasing out its provision of customer location information to aggregators. We made an exception for use cases involving emergency services and fraud prevention in order to avoid undue disruption to providers of such services given their potentially important public benefits. In that regard, there can be real, and potentially life-saving, benefits, when a towing company receives the location of a stranded motorist who does not know the nearest mile marker, or a son or daughter uses a medical alert device to locate an injured elderly parent; or a bank uses location information to thwart fraud and identify theft.

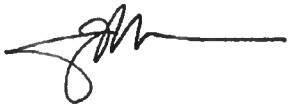
Even before this phase-out, AT&T limited its provision of location information to approved use cases and imposed strict standards to protect against improper use or disclosure of customer location data. Before we provided customer location data to an aggregator or location-based services ("LBS") provider, we investigated them – their corporate history, security policies, and privacy policies – and approved each planned use of customer location data. AT&T required the entity receiving customer location data to provide notice to customers of the intended use of their information and to obtain customers' consent for that use. We also required location aggregators and LBS providers to confirm a record of customer consent associated with each request for AT&T location data, and we reviewed those records daily. We also restricted the downstream dissemination of location information provided to location aggregators and LBS providers.

As of this date, AT&T is not aware of any instance in which the location information of one of its customers has been shared without authorization in connection with the incident described in your letter. Nonetheless, in light of the press report to which you refer, which did not involve an AT&T phone, we decided in January 2019 to accelerate our phase-out of these services. As of March 29, 2019, AT&T stopped sharing any AT&T customer location data with location aggregators and LBS providers. 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.

Lastly, we note that the media reports to which you refer regarding the legal requirements associated with A-GPS,[1] are inaccurate and misplaced. The FCC's prohibitions on the use of the National Emergency Address Database ("NEAD") for non-emergency services do not apply to A-GPS because A-GPS is not associated with or stored within NEAD.[2] Instead, the NEAD is being developed to include "MAC address and BT-PDA information of fixed indoor access points (e.g., Wi-Fi and Bluetooth) that will be used to determine the specific indoor location of wireless 911 callers...."[3] 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, ridesharing 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.

Please let us know if we may be of further assistance.

Sincerely,



Joan Marsh

cc:

[1] Karl Bode, *What A-GPS Data Is (and Why Wireless Carriers Most Definitely Shouldn't Be Selling It)*, MOTHERBOARD (Feb. 7, 2019), *available at* https://www.vice.com/en_us/article/j575dg/what-a-gps-data-is-and-why-wireless-carriers-most-definitely-shouldnt-be-selling-it.

[3] Federal Communications Commission, *In re Wireless E911 Location Accuracy Requirements*, Order 17-150 ¶

Brighter Future For All

May 15, 2019

VIA EMAIL

Jessica Rosenworcel
Commissioner
Federal Communications Commission
Washington, D.C. 20554
Jessica.Rosenworcel@fcc.gov

Dear Commissioner Rosenworcel:

Thank you for your May 1, 2019 letter to Michel Combes, Chief Executive Officer of Sprint Corporation ("Sprint"), regarding Sprint's location based services ("LBS"). In response to your questions, Sprint is currently only using one location aggregator to provide LBS 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. 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.

Sprint's commercial LBS platform does not have connectivity to, nor does it use data from, the National Emergency Address Database ("NEAD"). While the NEAD is not yet available for use with live 9-1-1 calls, the privacy and security protections adopted by the FCC proscribe use of NEAD data for commercial purposes. *See In re Wireless E911 Location Accuracy Requirements,* Memorandum Opinion and Order, 32 FCC Rcd. 9699, ¶ 3 (Nov. 14, 2017). Furthermore, the NEAD is populated with Media Access Control ("MAC") identifiers for certain Wi-Fi access points and their associated locations and does not contain location data from smartphones. *See* 47 C.F.R. § 20.18(i)(1)(ii)-(iii). While the Commission's regulations do not prohibit the use of MAC identifiers obtained independent of the NEAD, Sprint's commercial LBS platform does not rely on such data to derive location information.

Finally, Sprint's contracts with location aggregators have permitted aggregators to store location data for time periods, which allows for adequate response to any claims that may subsequently arise. These contracts require encryption and permit access to or disclosure of location data by the aggregator only as necessary to fulfill its obligations under the contract.

Thank you for the opportunity to address your questions.

Sincerely yours,

Maureen Cooney
Head of Privacy
Office of Privacy

T-Mobile

May 15, 2019

By email (Jessica.Rosenworcel@fcc.gov)

The Honorable Jessica Rosenworcel
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Response to Letter Dated May 1, 2019

Dear Commissioner Rosenworcel:

Thank you for your May 1, 2019 letter regarding T-Mobile's location aggregator program. T-Mobile takes the privacy and security of our customers' data very seriously. Therefore, we are grateful for the opportunity to provide clarity about our now-terminated program, and to correct several persistent misconceptions about its operations. In response to your question about the termination date, as of February 8, 2019, T-Mobile terminated all service provider access to location data under the program, and T-Mobile terminated its location-based service contracts with the Location Aggregators, effective March 9, 2019.

T-Mobile's former location aggregator program was always 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. Those services delivered numerous consumer benefits, including services like roadside assistance, medical emergency alerts, and bank fraud prevention.

The vendors who provided these services ("LBS providers") received T-Mobile customer location data through their contractual arrangements with LocationSmart or Zumigo, the two location aggregators under contract with T-Mobile (the "Location Aggregators"). T-Mobile governed access to location data by the Location Aggregators and their service provider customers through several important safeguards, including contracts, service use approvals, and periodic assessments conducted by an outside audit firm at the direction of T-Mobile's counsel.

These safeguards included contractual conditions that the Location Aggregators were, in turn, required to impose upon each downstream LBS provider. These provisions required compliance with CTIA's Guidelines for Location-Based Services, as well as a requirement to obtain the prior consent of each end-user (the consumer) for access to their location information.

Prior T-Mobile approval was required for any LBS provider and each location-based service to be offered, based on detailed information submitted by the Location Aggregators. This information included specific documentation of the customer notice and consent processes, including the LBS provider's proposed consent capture process. T-Mobile evaluated the proposed consent process 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.

T-Mobile also assessed its location aggregator program through periodic audits and reviews to ensure that these protections and safeguards were working properly. These reviews were designed to confirm, among other things, that LBS providers were only using the information after receiving affirmative customer consent.

It is important to emphasize that T-Mobile's Location Aggregators and the LBS providers did not receive T-Mobile customer location information in bulk or under contract terms that allowed access to geolocation information at their discretion. Rather, they were authorized to access customer location information only for specific uses approved by T-Mobile, and only upon an individual customer 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. T-Mobile's agreements with the Location Aggregators permitted the retention of customer geolocation information only for as long as business needs required and then mandated the destruction of the information. While those agreements are now terminated, provisions that survive termination establish that neither the aggregators nor any LBS providers may make further use of any location data acquired via this program.

Moreover, at no time during the existence of T-Mobile's location aggregator program did the Location Aggregators or the downstream LBS providers receive information derived from the National Emergency Address Database ("NEAD") or from 911 calls – the use of which is limited under federal law. In fact, the NEAD is still under development and has yet to be used in a true production environment. In addition, the NEAD will rely on commercially-deployed Wi-Fi Access Points and Bluetooth Beacons to derive an indoor location and will not be based on A-GPS-derived location information that is at the core of most commercially-deployed location based services.[1] And, while Assisted GPS ("A-GPS") data is important to current 911 functions, there appears to be a misconception in press reports that 911 services are its only source or use. A-GPS data is used by many popular third-party apps that, in turn, leverage the GPS capabilities in wireless devices and the publicly available GPS satellite data.

T-Mobile undertook an evaluation last summer of whether to retain or restructure its location aggregator program, in light of the Securus incident discovered last year.

---

[1] *See, e.g.*, http://www.911nead.org/.

Ultimately, we decided to terminate it. We notified the Location Aggregators on October 26, 2018, that we were terminating their contracts. T-Mobile agreed to a phased termination approach because we did not want to abruptly terminate location-based services that provided important consumer benefits, such as emergency assistance services, without giving customers an opportunity to find alternatives. Accordingly, as of February 8, 2019, T-Mobile terminated all LBS provider access to location data under the program. T-Mobile's location-based service contracts with the Location Aggregators officially expired on March 9, 2019.

Sincerely,

Kathleen O'Brien Ham
Senior Vice President, Government Affairs
T-Mobile US, Inc.

verizon

Karen Zacharia
Chief Privacy Officer

1300 I Street, NW, Suite 500 East
Washington, DC 20005
Phone 202.515.2529
Fax 202.336.7923
karen.zacharia@verizon.com

May 15, 2019

Commissioner Jessica Rosenworcel
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Dear Commissioner Rosenworcel:

I write in response to your May 1, 2019 letter to Hans Vestberg, Chief Executive Officer of Verizon. Verizon appreciates the opportunity to describe our practices with respect to location aggregators, to discuss how Verizon protects consumers' location information, and to explain the steps Verizon has taken to prevent misuse of that information. Verizon works hard to protect the privacy and security of our subscribers. With limited exceptions, we share personally identifiable subscriber location information only with the affirmative opt-in consent of a subscriber.[1] The location information sharing that you refer to in your letter relates to Verizon's prior location aggregator program,[2] outlined below, which allowed two third party aggregators to share location information of certain of our wireless subscribers at particular moments in time with their corporate customers under specific conditions (including having obtained consent from our wireless subscribers). Except for four roadside assistance companies, Verizon terminated its location aggregator program in November of 2018. And Verizon terminated the arrangements with the four remaining companies at the end of March 2019.

In our now-terminated location aggregator program, Verizon contracted with two aggregators, LocationSmart and Zumigo. Through that program, the aggregators shared location information allowing their corporate customers to provide a variety of location-based services, such as roadside assistance, call routing, and fraud prevention. The aggregators' corporate customers were required to obtain subscriber consent prior to requesting any location information. Verizon also had a detailed process for reviewing and authorizing the aggregators'

[1] As detailed in our privacy policy, https://www.verizon.com/about/privacy/privacy-policy-summary, Verizon also shares personally identifiable subscriber location information as required by law and with vendors and contractors who are acting on behalf of Verizon and who may only use the information for Verizon purposes. Except with the affirmative opt-in consent of a subscriber and as detailed in our privacy policy, Verizon does not share personally identifiable subscriber location information under any other circumstances.

[2] Verizon refers to its prior location aggregator program as its "Location Data Integration" or "LDI" service.

corporate customers and those customers were limited to using our subscriber location information for specific, approved use cases. Verizon also regularly conducted audits of the program through a third party auditor.

Our agreements with the aggregators authorized the aggregators to access subscriber location information, on behalf of their corporate customers, for the sole purpose of providing the services and as disclosed to and authorized by the subscriber. The terms also stated that location information could not be accessed, used, copied, stored, or disclosed for any other purpose without the explicit prior consent of subscribers. The terms required aggregators, and their corporate customers, to delete location information immediately when it was no longer needed and provide a readily available means for subscribers to subsequently opt out from sharing their location information at any time. These agreements required the aggregators to flow down these requirements to all of their corporate customers.

The location information that the aggregators received through Verizon's prior location aggregator program included the approximate latitude and longitude of the subscriber's mobile phone, as well as the error radius and other error information for location queries, and the date and time stamp for the location transaction. While the location aggregator program generally offered coarse location information, a small percentage of the location information provided through the aggregator program was more accurate location information. A-GPS data included in the National Emergency Address Database was not available to aggregators through the program. Similarly, location information associated with a 911 call was not available through the program.

Last June, Verizon committed to terminate our location aggregator program. We followed through on that commitment. As of the end of November 2018, Verizon had fully terminated its location agreement with one aggregator (Zumigo) and had terminated almost all access to location information by the corporate customers of the other aggregator in the program (LocationSmart). The only exception is that we maintained the prior arrangement with LocationSmart for four companies for the narrow use of providing roadside assistance during the winter months for public safety reasons. The arrangement for those remaining entities fully terminated at the end of March 2019. Those, and all other third-party, entities no longer have access to Verizon subscriber location information through the aggregators.

Thank you for your interest in this important matter.

Sincerely,

Karen Zacharia

Karen Zacharia
Chief Privacy Officer
Verizon
1300 I Street, NW – Suite 500 East
Washington, D.C. 20005