



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](mailto:karen.zacharia@verizon.com)

January 30, 2019

The Honorable Greg Walden  
The Honorable Cathy McMorris Rodgers  
The Honorable Robert E. Latta  
The Honorable Brett Guthrie  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Ranking Members Walden, Rodgers, Latta, and Guthrie:

I write in response to your January 16, 2019 letter to Hans Vestberg, Chief Executive Officer of Verizon. Verizon appreciates the opportunity to describe our practices with respect to location aggregators and direct location-based services, to discuss how Verizon protects consumers' location information, and to explain the steps Verizon is taking to prevent misuse of that information.

Verizon works hard to protect the privacy and security of our customers. As detailed below and in our privacy policy, we generally share personally identifiable customer location information only with the affirmative opt-in consent of a customer.<sup>1</sup> The location information sharing that you refer to in your letter relates to Verizon's prior location aggregator program,<sup>2</sup> 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). The Motherboard article referenced in your letter alleges that Microbilt obtained location information for other carriers' customers through those carriers' respective location aggregator programs. Verizon was not implicated in this article because Verizon terminated its own location aggregator program, with a narrow exception described below, in November of 2018.

---

<sup>1</sup> As detailed in our privacy policy, <https://www.verizon.com/about/privacy/privacy-policy-summary>, Verizon also shares personally identifiable customer 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. Verizon does not share personally identifiable customer location information under any other circumstances.

<sup>2</sup> Verizon refers to its prior location aggregator program as its "Location Data Integration" or "LDI" service.

## Verizon's Former Location Aggregator Services

Verizon contracted with two aggregators, LocationSmart and Zumigo, in our location aggregator program. 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. Under this program, the aggregators' corporate customers were required to obtain consumer consent prior to requesting any location information. Verizon also had a detailed process for reviewing and authorizing the aggregators' corporate customers and those customers were limited to using our customer location data for specific, approved use cases. Verizon also regularly conducted audits of the program through a third party auditor.

Last Spring, Verizon learned that Securus Technologies was obtaining location information from 3CInteractive through this program and using it for unauthorized purposes. Verizon immediately took steps to suspend Securus Technologies's and 3CInteractive's access to Verizon customer location information through LocationSmart. In addition, Verizon undertook a review to better understand how this issue could occur despite the contractual, auditing, and other protections we had in place in our location aggregator program to protect our customers' location data. As a result of this review, we decided to terminate our location aggregator program.

Verizon followed through on our commitment to terminate location aggregation agreements. 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 have 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, but those remaining entities all have agreed to transition out of the existing arrangements by the end of March 2019.

## Verizon's Direct Location Services

Verizon now offers a direct location-based service<sup>3</sup> to corporate customers, under which they may obtain location information for specific purposes like roadside assistance, fraud detection, and logistics and dispatch.<sup>4</sup> Under this new service, Verizon obtains the affirmative direct opt-in consent of its wireless subscribers to share their location information with a particular corporate customer. Specifically, when a corporate customer requests the location of a Verizon wireless customer, Verizon sends that wireless customer a text message asking if their location may be shared with the corporate customer. This text message identifies the party requesting the wireless customer's location information and the limited period of time (up to 30 days), if applicable, for which their consent will be valid.<sup>5</sup> Verizon also sends a confirmation

---

<sup>3</sup> Verizon refers to this new location-based service as its "Direct Location Service."

<sup>4</sup> Location used in Verizon's Direct Location Service is limited to coarse (rather than precise) location information. More precise location information, such as that which is available through GPS based on the device itself, is usually what customer-facing apps rely on to deliver consumer-oriented and approved location applications.

message to wireless customers once they have opted in and that message describes how they can withdraw consent if the consent is valid for longer than one-time. If the wireless subscriber responds affirmatively, Verizon will share their location information with the requesting corporate customer. If not, Verizon will not share that information.

Verizon has other protections in place as well to ensure the wireless customers' location information is protected. Verizon has established a clear set of preapproved and authorized use cases for its corporate customers and screens those corporate customers to ensure that they have not violated federal or state law or rules related to consumer protection and consumer privacy. Verizon also regularly conducts audits to ensure that its corporate customers are still in compliance with our supplier integrity standards.

### The Motherboard Article

Verizon was not implicated in the Motherboard article that you reference in your letter. As you know, Motherboard claimed that its reporter successfully hired a bounty hunter to find the location of a particular individual. In that particular instance, the article states that T-Mobile provided its wireless customer's location information to Zumigo; Zumigo then provided it to Microbilt; Microbilt then provided it to a bail bond company; the bail bond company provided it to the so-called bounty hunter; and the bounty hunter then provided it to the reporter. The article claimed that AT&T and Sprint had similar arrangements that would allow this type of location sharing. The reporter, however, was not able to obtain location information about Verizon's customers in this way because Verizon terminated its location aggregator agreement with Zumigo (the aggregator involved in the Microbilt situation with other carriers) at the end of November 2018. Today, under Verizon's new direct location services, a bounty hunter would not be able to gain unauthorized access to Verizon's wireless subscriber location information because we send a text message directly to the wireless subscriber asking them to consent to the sharing of location information.

### Questions/Answers

The answers to your specific questions are below. The premise of the majority of these questions no longer applies to Verizon since we are moving to a direct model under which we control, ensure, and record that our end users consent directly via text message to the sharing of location information. Unless otherwise noted, our responses are limited to the location aggregator program that Verizon has largely terminated.

- 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?**

Verizon notified Zumigo in June 2018 that it was terminating its relationship with them as a location aggregator and completed that termination at the end of November 2018. Zumigo is thus no longer able to access location information from Verizon.<sup>6</sup>

---

<sup>5</sup> If the consent is valid only for one-time access, the timeframe is not listed.

In addition, as noted above, Verizon has launched a direct location service in which we obtain the consent for any location sharing directly from our wireless subscribers through text messages. Verizon's corporate customers who purchase this service may ultimately use Zumigo or another third party to help them integrate with Verizon's location platform. Notwithstanding their integration efforts, Verizon provides the location information of its wireless subscribers directly to the corporate customer, not to Zumigo or other location aggregator or third party, and only after Verizon obtains the consent directly from our subscribers.

**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?**

Verizon notified LocationSmart in June 2018 that it was terminating its relationship with them as a location aggregator. Verizon terminated LocationSmart's access to location information for almost all of its corporate customers at the end of November 2018. The only exception is that we temporarily have maintained the prior arrangement for four roadside assistance companies during the winter months for public safety reasons. These companies asked Verizon for more time because they needed that time to transition off of their existing arrangements and services. They have all agreed to transition out of the existing arrangements through LocationSmart by the end of March 2019.

Verizon does not – and never had – any contracts with 3CInteractive or Securus Technologies for location information. Instead 3CInteractive and Securus Technologies gained access to Verizon customer location information through LocationSmart. Verizon terminated 3CInteractive's and Securus Technologies' access to location information through LocationSmart in May 2018. Neither 3CInteractive nor Securus Technologies currently has access to location information from Verizon.

In addition, as noted above, Verizon has launched a direct location service in which we obtain the consent for any location sharing directly from our wireless subscribers through text messages. Verizon's corporate customers who purchase this service may choose to use LocationSmart or another third party to help them integrate with Verizon's location platform. Notwithstanding their integration efforts, Verizon provides the location information of its wireless subscribers directly to the corporate customer, not to LocationSmart or other location aggregator or third party, and only after Verizon obtains consent directly from our customers.

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

---

<sup>6</sup> Verizon has an agreement with Zumigo under which Zumigo may act as an aggregator and access non-location information, such as contact and device information, in certain specific instances. This program does not include location information.

Verizon shared personally identifiable location information with LocationSmart and Zumigo through its location aggregator program. Verizon currently shares personally identifiable location information with eight companies through its direct location services program, only after we have obtained the text message consent of our end users for the sharing of the information.

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

The two location aggregators Verizon dealt with had access only to location information through the location aggregator program. The location information they received included the customer's latitude and longitude, as well as the error radius and other error information for location queries, and the date and time stamp for the location pull. No other customer information was available to the location aggregators through the location aggregator program.<sup>7</sup>

**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.**

The location aggregators were authorized to provide the same information described in response to question no. 4, above, to each of their corporate customers provided that (a) the relevant wireless subscribers had consented to the location sharing, (b) the corporate customers were previously authorized by Verizon, and (c) those corporate customers were using the information as authorized (*i.e.*, for the specified, approved use cases).

**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 [it] 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?**

Under the location aggregator program that Verizon is terminating, the aggregator's corporate customers were required to obtain the Verizon subscriber's consent prior to accessing the location information. Without consent, the aggregator was not permitted to share location information for that mobile device with its corporate customer. A record of this consent, the mobile device number, and the time stamp for the location request were sent to Verizon's auditor for daily review.

**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 service?**

---

<sup>7</sup> The location aggregators may receive non-location information, such as contact and device information, from Verizon in other ways and through other programs.

As part of the location aggregation program that we are terminating, Verizon built contractual provisions into its arrangements with the location aggregators that required affirmative customer consent, compliance with consumer protection and data privacy laws, and compliance with industry best practices. Under the agreements, Verizon also was permitted to terminate any arrangement that failed to meet our standards. For example, Verizon immediately terminated 3CInteractive's and Securus Technologies' access to location information through LocationSmart as soon as Verizon became aware that they were misusing the information they had obtained.

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

Prior to Verizon announcing that it planned to terminate its location aggregator program last year, the aggregators collectively were providing services to approximately 75 customers. We have terminated the arrangements involving all but four of those customers, and the remaining four will be terminated by the end of March 2019 (as explained above).

**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?**

See our response to Question 7.

**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?**

Under the legacy location aggregator program, Verizon required the location aggregators to obtain approval from Verizon before sharing location information with any of their corporate customers. Verizon also followed up by regularly conducting audits through a third party auditor to ensure that a location aggregator's customers were complying with our requirements. This audit process, however, did not reveal that 3CInteractive/Securus Technologies was using this information in ways that differed from their approved use case with LocationSmart. The audit likely did not alert our auditor to a potential problem because (i) 3CInteractive/Securus Technologies was using its profile for an approved use case to access location information for unauthorized purposes; (ii) nothing changed in the background check that the auditor maintains for 3CInteractive/Securus Technologies that would have prompted the auditor to question the credibility about following approved use cases; and (iii) the number of requests from 3CInteractive/Securus Technologies was consistent with the number the auditor normally would expect from them. Our review of this experience prompted us to decide – and to follow through – on terminating our location aggregator program and move to a model under which we directly control the consent process.

**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?**

Verizon has conducted regular meetings with its auditor to discuss monitoring of the program. The auditor processes location and consent records on a daily basis to monitor location transactions and reports upon any anomalies. In addition, Verizon undertakes a regular review of customer use with our auditor to confirm that the aggregators' corporate customers continue to meet Verizon and industry standard best practices. Verizon regularly reviews our auditor's "secret shopping" programs to validate continued adherence to program guidelines. And, as noted above, Verizon largely has terminated the program – which will be wound down completely by March 2019.

**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?**

Verizon used the third-party auditor, Aegis Mobile LLC.

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

Verizon largely terminated its location aggregator program at the end of November 2018. As discussed above, the only exception is that we have maintained the prior arrangement with LocationSmart for four roadside assistance companies during the winter months for public safety reasons, but those four remaining corporate customers have agreed to transition out of the existing arrangements by the end of March 2019.

**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?**

See our response to Question 10.

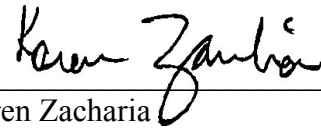
**15. Is Verizon aware of any other incidents of inappropriate or unlawful use of location information through a location aggregator or another third party since 2007?**

Due to the passage of time, Verizon is limiting this response to the last three years. Aside from the 3CInteractive/Securus Technologies incident, Verizon learned last May that a cybersecurity researcher was able to gain access to Verizon customer data through LocationSmart's website via a demonstration page for prospective customers. LocationSmart disabled the demonstration site immediately after learning of this vulnerability. LocationSmart also confirmed that the researcher attempted location queries only for individuals who had first given him their consent. And LocationSmart further confirmed that the vulnerability that allowed the researcher to access this information was not exploited by anyone else prior to the researcher's activity on May 16, 2018, and thus did not result in any mobile users' information being obtained without their permission.

\*\*\*\*\*

Thank you for your interest in this important matter. We are committed to protecting the privacy and security of our customers' location information. We recognize that location information can provide many pro-consumer benefits but we must protect that data from unauthorized access and use. Our customers' trust and comfort surrounding the use of location information will remain paramount, and we plan to act accordingly.

Sincerely,

A handwritten signature in black ink that reads "Karen Zacharia". The signature is written in a cursive style and is positioned above a horizontal line.

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