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

June 15, 2018

Hon. Ron Wyden
U.S. Senate
221 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Wyden:

I write in response to your May 8, 2018 letter to Lowell C. McAdam, Chairman and Chief Executive Officer of Verizon. Verizon appreciates this opportunity to describe our practices with respect to location aggregators, to discuss how Verizon protects consumers' location information, and to explain the steps Verizon is taking to prevent misuse of that information going forward.

Verizon takes the privacy and security of customers' information seriously. 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.[1] The location information sharing that you refer to in your letter relates to Verizon's location aggregator program,[2] which allows two third party vendors to share location information of our customers with their corporate customers under specific conditions. This program permits the corporate customers to obtain location information for specific purposes like fraud detection or customer identification among others. As part of that program, we require that the aggregator or corporate customer obtain consent from Verizon customers before they can receive location information.

In addition, we also require that any company who participates in the program access customer location information only for specified purposes, go through a detailed review and authorization process, and be audited regularly to ensure the information is being accessed only with customer consent and as authorized. In the case of Securus Technologies, as soon as we determined that Securus was accessing location information for unauthorized purposes, we immediately blocked Securus's access to customer location information through our vendor LocationSmart.

---

[1] 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.

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

It is against that backdrop that we conducted a comprehensive review of our location aggregator program. This review was in addition to the regular monitoring and ongoing audits Verizon undertakes throughout the use of location aggregation services in our location aggregator program. As a result of this review, we are initiating a process to terminate our existing agreements for the location aggregator program.

Location-Based Aggregation Services

Verizon contracts with two aggregators, LocationSmart and Zumigo, in our location aggregator program. These aggregators in turn provide a variety of location-based services to their corporate customers. For example, these location aggregators may use certain kinds of Verizon customer location data[3] to route a customer's call to the correct service location or to verify a customer's identity to prevent fraud. Truck rental companies may use the location data to provide better assistance to customers renting trucks who experience problems on the road. And financial institutions use location services to approximate a user's proximity to their home address when applying for a credit card online to help confirm their identity and reduce fraud. The end users of these corporate customers in many cases view these as helpful services and must affirmatively consent to the use of their location data.

Customer Protections

We have girded the pro-consumer aspects of these services with mechanisms designed to protect against misuse of our customers' location data. Consent by our customers is the cornerstone: we require clear notice to customers regarding who is accessing their information and how it will be used, and a Verizon customer must provide affirmative consent before the location aggregator may access that customer's location. Verizon has established a clear set of preapproved and authorized use cases for the location aggregators and their customers. Verizon screens the location aggregator's customers before approving their access to location services to ensure these customers have not violated federal or state law or rules related to consumer protection and consumer privacy.

Verizon's oversight does not end upon approving a customer. Instead, Verizon follows up by regularly conducting audits through a third party auditor to ensure that a location aggregator's customers are (i) obtaining the requisite customer consent prior to accessing and using customer location information and (ii) still in compliance with our supplier integrity standards.

In addition, Verizon has built contractual provisions into its arrangements with location aggregators that require affirmative customer consent, compliance with consumer protection and data privacy laws, compliance with industry best practices, and the ability to terminate any arrangement that fails to meet our standards.

---

[3] Location data used in the location aggregator program is limited to coarse (rather than precise) location information. As its name implies, precise location information is more specific and is the type available through GPS based on the device itself. That more precise information is usually what customer-facing apps (e.g., mapping or car services) rely on to deliver consumer-oriented and approved location applications. Coarse location information is derived from the Verizon network and is significantly less accurate than precise location information.

Securus's Unauthorized Use

Despite the protections that Verizon built into its location aggregation arrangements, it appears that Securus and/or its affiliate 3C Interactive impermissibly permitted law enforcement agencies to request location information through LocationSmart for investigative purposes. 3C Interactive/Securus was an approved third party for the location aggregator LocationSmart to access Verizon customer location information for its law enforcement customers for one purpose: to confirm that call recipients were not within a certain distance of the prison from which a collect phone call was placed. Use of location information for investigative purposes was not an approved use case in our agreement with LocationSmart. So, once the issue was identified, Verizon immediately took steps to suspend Securus's and 3C Interactive's access to Verizon customer location information through LocationSmart.

We 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. Our preliminary conclusion is that our regular audit did not reveal that 3C Interactive/Securus was using this data 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 was using its profile for the approved use case to access location information for unauthorized purposes; (ii) nothing changed in the background check that the auditor maintains for 3CInteractive/Securus that would have prompted the auditor to question its credibility about following approved use cases; and (iii) the number of requests from 3CInteractive/Securus was consistent with the number the auditor normally would expect from them.

Next Steps

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 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.

Questions/Answers

The answers to your specific questions are below. Our responses are limited to the location aggregator program described above through which Securus obtained access to certain customers' location information.

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.**

Verizon contracted with two location aggregators, LocationSmart and Zumigo, that offer services that allow individual mobile phone users to share their location with specific businesses for specific purposes. Verizon has authorized these location aggregators to facilitate access to Verizon customer location information only after the aggregator or their customer has obtained the affirmative opt-in consent of the wireless customer. In addition, these aggregators may facilitate access to customer location information only for approved use cases. For example, location information is used to locate and dispatch roadside assistance to wireless customers, to optimize the supply chain and workflow of a business, to provide visibility into the status of jobs and deliveries, and to authenticate customers to prevent fraudulent activity and secure online transactions. The location aggregators collectively provided these services to approximately 75 customers.

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

The location aggregators have access only to "coarse" location information. They do not have access to more precise location information derived from GPS and other more precise location technologies. The coarse location information they may receive includes the customer's approximate latitude and longitude, as well as the error radius and other error information for location queries. For example, the aggregator could determine that a customer that has given them consent is around 1000 meters from a particular location. No other customer information is available to the location aggregators through this location aggregator program.[4]

Under this program, either the aggregator or the aggregator's customer must obtain the Verizon user's consent prior to accessing the location information. Without consent, the aggregator may not grant access location information for that mobile device. A record of this consent, the mobile device number, and the time stamp for the location request are sent to Verizon's auditor for daily review.

[4] These aggregators may receive non-location information, such as contact and device information, from Verizon in other ways and through other programs.

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.**

Each aggregator is required to submit a request for access to location information for each of their customers. These submissions include the consent process used by the aggregator or the customer and must be limited to the pre-determined set of use cases. Verizon vets and reviews all the requests. In addition, Verizon's outside auditor regularly monitors the aggregators and their customers to ensure they continue to comply with Verizon's program requirements. As explained above, our outside auditors receive records detailing the location information that was provided to each customer and the associated consents on a daily basis for review.

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.**

Verizon did not uncover any new incidents in which a location aggregator or customer of a location aggregator misrepresented that they had customer consent during the investigation that we launched upon learning of the incident with Securus. We did learn recently, though, 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 has 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. Verizon also confirmed that our other location aggregator, Zumigo, does not maintain a demonstration site, and we directed both LocationSmart and Zumigo to not use Verizon customer data in any demonstration site going forward.

To the extent Verizon is aware of any prior incidents, they were addressed and resolved.

****

Thank you for your interest in this important matter. We are committed to protecting the privacy and security of our customers' location information, and will keep you informed as we execute our plan to terminate these location-based aggregation arrangements with the aggregators.

We recognize that location information can provide many pro-consumer benefits. But our review of our location aggregator program has led to a number of internal questions about how best to protect our customers' location data. We will not enter into new location

aggregation arrangements unless and until we are comfortable that we can adequately protect our customers' location data through technological advancements and/or other practices. Our customers' trust and comfort surrounding the use of location information will remain paramount, and we plan to act accordingly.

Sincerely,

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