



June 15, 2018

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Wyden:

Thank you for your May 8, 2018 letter to Marcelo Claure, Executive Chairman of Sprint Corporation (“Sprint”), regarding Sprint’s location based services (“LBS”). Sprint takes its obligations to safeguard our customers’ privacy seriously, and does so in a number of ways with respect to LBS. Sprint implements CTIA’s Best Practices and Guidelines for LBS, and requires compliance with the same in contracts related to LBS. Account holders or end users must generally be notified about how their location information will be accessed, used, and disclosed so that they can make an informed decision about whether to provide their consent. There are certain instances, however, such as with child safety, when the account holder (*e.g.*, parent), rather than the end user (*e.g.*, child), receives notice and provides consent because of the nature and special circumstances of these types of services. Sprint also responds to lawful demands for location information in response to government investigations, in which case notice to the account holder or end user is prohibited or not required.

Sprint is pleased to answer your questions below specifically with respect to LBS.

- 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.**

Sprint generally offers three types of LBS products for business end-users. These include (1) fleet management (*e.g.*, tracking a cargo truck); (2) asset management (*e.g.*, tracking a product for delivery); and (3) people tracking (*e.g.*, GPS bracelets for parolees). Depending on the product, Sprint may provide location information to vendors, application developers, and location aggregators, who in turn provide the information to the ultimate end-user.

Sprint additionally offers *Safe & Found*, a mobile security application that allows a “family” to be set up with one “parent” and up to five “child” members that can be from other carriers. All family members can view each other’s locations on a map and set up safety areas so other members can receive notifications when members leave those areas. Users can also locate

a lost or stolen device and remotely lock it. Sprint uses a vendor for this service to obtain opt-in consent from the account holder and process location information.

Sprint's Mobile Advertising Program also provides the opportunity to have Sprint and its advertising partners provide ads that are more relevant to a customer's interests. This program is only available to customers who have provided opt-in consent. Under this program, Sprint shares de-identified information with its advertising partners that consists of an anonymous identifier associated with the customer's mobile device together with location information.

Examples of other third-party applications to which users may opt in and that involve location sharing with location aggregators include: roadside assistance to identify where customers are located; state traveler assistance systems used by governmental entities for two-way communications with the public during emergency events while traveling on state roadways; workforce applications that allow employees to check-in and check-out of job sites via SMS so that dispatchers can optimize schedules based on the location of their workforce; store finder applications that use the location of a caller's mobile device to provide a list of nearby stores and their locations to the caller; tax applications that help users track the number of days they spend in different tax jurisdictions; online gaming platforms run by state lotteries where the user's mobile location is obtained to confirm the user is in state.¹

- 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.**

Application developers and location aggregators are contractually obligated to incorporate conspicuous and standalone notice as part of the registration process for each LBS application that explains how location information will be accessed, used, stored, disclosed or collected. The end user must expressly and affirmatively accept the notice before continuing.

For applications where only the end user will see their own location information, the notice must be provided to, and consent must be obtained from, the end user.

For applications where a business account holder will have the ability to see location information regarding devices under its own account, the notice must be provided to, and consent must be obtained from, the account holder. End users of the devices under the account holder's account also must be notified in a clear and conspicuous manner that they may be located using the application.

For all other types of applications, Sprint's contracts require that the notice must be provided to, and consent must be obtained from, the end user who is registering for the

¹ In response to the concerns you noted in your letter of May 8, 2018, Sprint began an investigation. We suspended the provision of location data to Securus, and our investigation continues.

application. A notice must be provided to the account holder that the registrant has subscribed to a service that will locate the registrant's device. The developer must send an SMS message to the registrant's device promptly after registering to confirm the registration, and then send random periodic SMS messages to the registrant's device to remind the user that their device may be located.

Aggregators and developers must clearly and completely document the presentation of the above-referenced notices and any corresponding consent. Their records must include: (i) an identifier linking the end user to the record; (ii) a time and date stamp of the end user's acknowledgment; (iii) a reference to the version of the notice that was presented; and (iv) a developer application identifier.

- 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.**

Sprint receives consent for its *Safe & Found* application and Mobile Advertising Program directly or through its vendor.

For other applications, aggregators and developers must make the records described above available to Sprint upon request in a format specified by Sprint. For each network-initiated application, the aggregator is contractually obligated to provide the notice record to Sprint before Sprint provides location information to the aggregator.

For self-service LBS applications where the end user's location information is accessible by someone other than the end user (*e.g.* the developer, a tow truck company), the developer must maintain verifiable records (data log or voice log) of each instance of the end user's request to use the service. The log must be made available to Sprint upon request in a format specified by Sprint.

Sprint has the right to audit performance of the obligations described above, which includes seeking reports, full and complete access to relevant facilities, books, records, procedures, and information to assess compliance. Sprint maintains the contractual right to immediately suspend or terminate access to location information for reasons that include a breach of these obligations.

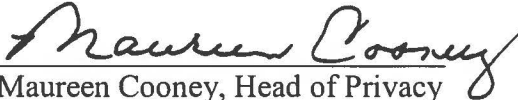
- 4. Please describe any incidents known to your company or uncovered during your responses to the above in which a third party with which your company shared customer data misrepresented that they had customer consent.**

Sprint is cautious with respect to alleging any intentional misrepresentation by third parties, but to protect its customers Sprint will continue to maintain its contractual rights and remedies to ensure third party LBS providers fulfill their obligations as described above.

The Honorable Ron Wyden
June 15, 2018
Page 4

Thank you for the opportunity to address your questions.

Sincerely,


Maureen Cooney, Head of Privacy
Office of Privacy