



April 19, 2011

Honorable Edward Markey
Honorable Joseph Barton
Co-Chairmen Bipartisan Privacy Caucus
House of Representatives
Congress of the United States
Washington, D.C. 20515

Dear Representatives Markey and Barton:

Thank you for your March 29, 2011 letter to Dan Hesse, CEO of Sprint Nextel Corporation (Sprint), seeking information on Sprint's privacy practices with respect to personally identifiable information and location data. Sprint understands that your interest arises from an article about telecommunications carrier Deutsche Telekom's practices in Germany that were highlighted in an article in the New York Times on March 26, 2011, and particular concerns that the article raised about tracking customer location.

Sprint does not engage in "tracking" its customers. It is important to understand, however, that user handsets must register their presence on a cell site in order for the network to properly route or deliver a call. Device registration is integral to being able to comply with the statutory and regulatory scheme in the United States that carriers must follow in delivering telecommunications services. Registration data is generally ephemeral and not stored for more than a few hours, unless necessary in particular instances to evaluate network performance or comply with regulatory requirements. Switch and cell site information associated with an actual call is retained for a longer period to comply with regulatory requirements and provide service-related functions, such as billing. Again, the retention of this information – which is protected by statute as described below – is not used for "tracking" users either. Finally, location applications offered by Sprint or third parties may rely on knowing the user's location to respond to a request. These services are offered by Sprint on an opt-in basis after full notice.

Consumers want and expect wireless services to be delivered in a seamless manner continuously, 24-7, regardless of their location or whether their own provider has network services available or must roam on the network of another carrier. Registration of a device with the mobile network permits the delivery of requested customer

services and is necessary in order to comply with regulatory requirements, including those associated with E-911 service, carrier interconnection compensation, and roaming, as well as the protection of customer proprietary network information.

Sprint is committed to its consumer and business customers and their satisfaction in our delivery of innovative products and services that meet their current and evolving needs. A key component to delivering on that commitment is respecting and protecting the privacy and security of each customer's personally identifiable information and other customer data. Sprint's privacy practices are constantly subject to internal review and evolve to meet and address a continuously changing wireless environment. Sprint also has been recognized and received accolades from the International Association of Privacy Professionals for innovation in building privacy into the internal compliance practices of our company.

Sprint has a dedicated, long-existing Office of Privacy. A multidisciplinary team of Sprint privacy professionals works across the enterprise, teaming with the Information Technology Department, Corporate (including network) Security, Product Design, Marketing and Sales, among others, to build privacy and risk mitigation into the design and delivery of Sprint services. Our efforts to protect customer privacy are iterative and both anticipate and respond to privacy risks and changes in technology. Our aim is to communicate well with our customers about our information privacy practices, provide consumers with choices about their data use, and be accountable for the use and protection of their information.

Question 1: Please describe the policies and procedures Sprint utilizes to comply with Section 222 of the Communications Act, which requires express prior authorization of the customer for use, disclosure of, or access to the custom's location information for commercial purposes.

Section 222 of the Communications Act requires that carriers protect the confidentiality of Customer Proprietary Network Information ("CPNI"),¹ which includes call location information derived from a consumer's use of a telecommunications service. 47 U.S.C. § 222. Under the Federal Communications Commission's (FCC) regulations, carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. 47 C.F.R. § 64.2010(a). Sprint employs administrative, physical and technical safeguards designed to protect CPNI from unauthorized access, use and disclosure. Further, Sprint requires customer approval before disclosing a customer's CPNI – including location information – to any third party, except as permitted under Section 222 or the FCC's regulations. *See e.g.*, 47 U.S.C. § 222(d).

¹ Customer Proprietary Network Information is "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." 47 U.S.C. § 222(h) (1).

Sprint also is a signatory to, and participated extensively in the establishment of, the CTIA Best Practices and Guidelines for Location-Based Services (“LBS”).² These industry guidelines require that notice be provided and consent obtained before using or disclosing location information; they apply to all commercial services where location information is linked by an LBS Provider to a specific device or person.

Consistent with Section 222 and the CTIA Best Practices and Guidelines, Sprint requires that consumers be given a notice (generally on the device itself) and that opt-in consent be obtained to use and/or disclose a customer’s location data when a commercial LBS is initiated. For network-based LBS, Sprint manages and records this consent process through its Location Gateway, which is a platform Sprint developed to enable the communication of incoming requests for location information and outgoing responses to those requests. An example of a network-based LBS that Sprint provides is Sprint Family Locator, which allows an accountholder (e.g., parent) to locate devices under his/her account (e.g., kids). When a parent locates a child’s device through this application, the location request comes into Sprint’s Location Gateway, which checks for a consent record before returning the location information.

For device-based LBS, the operating system on the device stores the consumer’s consent provided at application download. An example of a Sprint-provided device-based LBS is “Sprint Navigation,” an application that provides voice-guided driving directions, maps and traffic alerts on the mobile device. When a Sprint subscriber installs this application on his or her device, the subscriber is presented with an on-device notice and has the option of providing consent for Sprint to access the device’s location to enable the application by choosing “allow” or “don’t allow” (or some variation thereof, depending on the operating system of the device). When a subscriber chooses “allow,” this consent is stored within the operating system on the handset. Once consent is recorded, the operating system allows the application to request location information from the device’s GPS and sometimes from Sprint’s network if assistance data is needed.

In both instances – regardless of whether the LBS application is network or device-based – subscriber consent is obtained and recorded before Sprint uses or discloses the location information.

² CTIA is an international organization representing the wireless communications industry. CTIA advocates on behalf of its members at all levels of government. The association also coordinates the industry’s voluntary best practices and policy and education initiatives.

Question 2: What personally identifiable information does your company collect from its customers?

'Personally identifiable information', 'personal information', and 'personal data' are subject to varying definitions under state data breach laws, federal laws, federal guidance documents, and in international contexts. For purposes of Sprint's responses, we consider 'personally identifiable information' as information that alone or in combination identifies a particular individual. The personally-identifiable information that Sprint collects from its customers includes contact information (e.g., customer name, address, email address, home/work phone numbers); social security number; date of birth; credit/debit card information; banking account information (for automatic payments); location information; device information (serial numbers, type of device); and usage information (type and amount of usage of our services). This definition does not include anonymized or de-identified aggregate data. Please also see Sprint's privacy policy at www.sprint.com/legal/privacy.

Question 3: How is this information collected (i.e., initial sign-up process, usage of mobile phone, etc)?

Sprint collects personally identifiable information through a variety of customer touch points (e.g., Sprint's website, retail locations, call centers, via customers' devices) but through two primary methods: 1) customer-provided information and 2) customer usage of Sprint's device and services.

During initial sign-up, Sprint collects information necessary to initiate and bill for service through its application process; this information is collected directly from the customer. During a customer's term of service, Sprint collects additional information directly from customers for account maintenance, troubleshooting, etc.

Additionally, Sprint collects information from customers through customers' use of our services and applications. For example, while a customer is using a device, Sprint will collect information on the type of service the customer is using (data or voice); customer proprietary network information, including call detail information; and data usage information. We also collect information about the wireless device a customer is using, such as how the device is functioning, signal strength, and location of the device. This information helps Sprint to perform quality control functions on our network, and comply with federally-mandated regulations, including E-911 obligations and assurance of proper compensation to other carriers with whom we interconnect.

Question 4:

- a. ***How does your company use customers' personally identifiable information?***

Sprint uses customers' personally identifiable information for a variety of purposes, including to: provide products and services to our customers; protect Sprint's and our customers' rights and property; develop and market new products and services; customize or personalize customers' experiences with Sprint's services; provide personalized advertising and communications to customers; and monitor, evaluate, and improve our services, systems, and networks (i.e., network performance and speed, ability of a device to utilize network services,), as well as to respond to legal process and emergencies.

- b. ***Does your company rent or sell the information?***

Sprint does not rent or sell our customers' personally identifiable information. Sprint requires customer consent before providing personally identifiable information to third parties for their own use. For example, Sprint provides personally identifiable information to third-party application providers from whom a Sprint customer has downloaded an application and agreed to related terms and conditions.

- c. ***Does your company use personally identifiable information for marketing purposes?***

Yes, Sprint does use certain personally identifiable information for marketing purposes. Sprint uses customer contact information in its direct marketing efforts. Sprint also is permitted under Federal law to use customer proprietary network information ("CPNI") to market services and products within the categories of services to which a customer already subscribes. For instance, Sprint may use information about a wireless subscriber's usage of our voice services (e.g., minutes used per month) to market a particular rate plan that better meets that customer's needs (e.g., to refer customers to products that better reflect use patterns for their families, e.g., Sprint Family Services (www.sprint.com/family), to avoid overage fees or potential 'bill shock').

Further, while not personally identifiable information, with appropriate notice and an opportunity for consumer choice, Sprint uses information about our customers' use of Sprint-billed products and services to tailor advertising and communications to subscribers based on their interests.

Question 5:

a. How does your company store this information (i.e., in a form that is encrypted or otherwise indecipherable to unauthorized persons)?

In compliance with several state laws, Sprint encrypts certain personally identifiable information in transmission to any network outside of Sprint's own network (e.g., to a vendor). Within our data environment, Sprint utilizes both encryption and up-to-date methods and procedures to ensure data security. When it is not feasible or technically possible to encrypt personally identifiable information in storage, Sprint ensures the security and confidentiality of customer personally identifiable information through a series of controls that surround our data environment.

Sprint uses logical access controls at the operating system, database, and network layers to restrict access to customer information to those individuals that have a need-to-know such data. Access at the network layer is terminated when an employee's or contractor's relationship with Sprint terminates.

Database access is reviewed quarterly to ensure compliance with access control policy and procedures. On the periphery, Sprint has implemented a host of IT security measures to prevent intrusions. For example, firewalls have been implemented at all points of entry to Sprint's network, and intrusion detection systems are maintained at all Internet points of entry. Sprint has a centralized Security Department responsible for oversight of security policy, ensuring awareness of risks and enforcement of data security practices throughout the company. Sprint continuously reassesses its technology and processes to ensure that the security of customer data remains robust.

Additionally, Sprint complies with the Payment Card Industry Data Security Standard, governing the handling of sensitive payment card data related to consumer transactions.

b. How long is it stored?

Data retention is governed by an enterprise-wide data retention schedule. Categories of data are retained for varying lengths of time depending on the type and sensitivity of data, the applicable laws and regulations governing the retention of such data, the business purpose of the data and whether any of the data is subject to a legal hold requirement (i.e., due to ongoing litigation). Generally, basic customer account information is stored for the life of the account plus 3 years. Requests for location data processed through the Sprint Location Gateway (described in Sprint's response to Question 1) are logged and retained in an unreadable format for 2 years, but no actual location data (latitude/longitude coordinates) are included in those records.

c. How does your company dispose of the information?

Sprint handles disposal of customer information in several ways. Some Sprint systems that contain electronic records have automatic document deletion processes; others require manual deletion at the end of the data retention period (described above). Sprint's Record Compliance Policy requires that all sensitive information be destroyed such that the information cannot be practicably read or reconstructed for any purpose, and that reasonable measures are taken to protect against unauthorized access to or use of the sensitive information in connection with its disposal. These information destruction processes apply to paper, microfiche, disks, disk drives, tape and other destructible electronic or digital media containing sensitive information. In addition, vendors who store customer information on Sprint's behalf must return or destroy data (and certify such destruction has taken place) at the end of the contract term.

d. Is the information always disposed of after the customer has terminated his or her business relationship with the company? If not, why not?

Personally identifiable information is not always disposed of when a customer's relationship with Sprint ends. Sprint must retain data for legal, regulatory, and business purposes. Data is retained after the customer relationship has ended only if Sprint has a legitimate business purpose for retaining such data. For example, Sprint preserves records pursuant to various state statutes of limitations for purposes of contract or other claims that may arise after termination of the customer relationship. As noted at response 5(b), basic customer account information is generally stored for the life of the account plus 3 years.

Question 6: Other than pinpointing a customer's location for purposes of identifying the strongest signal, does Sprint use any other mechanisms for determining the location of a customer's mobile phone, such as how frequently the customer checks her email? If yes, what are these mechanisms and what is the purpose of each of them?

Generally, there are two methods by which Sprint locates a device operating on its network. The first is through cell site and sector registration information (i.e., at which cell site the device was last registered). The second is through GPS technology embedded in the mobile phone.

When a Sprint subscriber uses her mobile phone to check or send email, she is using Sprint's data network and the device is registered with a cell site for that session. Cell site location information is necessary to provide the data services (i.e., email), just as it would be to provide voice service. Sprint generally does not use that information outside of providing the service and for compliance with regulatory requirements, such as data roaming and related intercarrier compensation requirements.

Outside of the commercial location-based services and applications requiring express customer consent (discussed in Sprint's response to Question 1), Sprint may collect customers' location information, as permitted by law and as consistent with our privacy policy notice, for reasons such as complying with the FCC's requirement to provide location information about our customers for the provision of E-911 services; identifying dropped calls; identifying malfunctioning devices; and planning future cell tower locations. Sprint uses a combination of handset-based and network-based mechanisms to comply with the FCC's requirements and carry out these other location-related functions.

Question 7: Is it a common practice of your company to inform the customer when relevant data is being collected and how this data is being used? If not, why not?

Yes, Sprint's practice is to inform and educate our customers when information about them is being collected and how it is being used. We use various methods of communications to educate and inform our customers, including:

- 1) Sprint's posted Privacy Policy available on our website, www.sprint.com/legal/privacy;
- 2) additional online notices related to certain activities on www.sprint.com that collect or use personally identifiable information;
- 3) periodic direct notices to customers via their monthly invoice or via direct mail, email or SMS message;
- 4) on-device notices regarding the download or use of certain applications that collect personally identifiable information; and
- 5) notices that are included with printed materials contained within the handset or device packaging.

Below are some examples of each privacy communication method and how Sprint uses it to keep customers informed about its data collection and use practices.

- Sprint's Privacy Policy is available online at www.sprint.com/legal/privacy (and under the "Privacy Policy" link in the footer of Sprint's homepage). It informs the customer of the various ways that we collect and use personal information. Any page on Sprint.com or on a Sprint handset where we solicit or collect customer information also includes a direct link to this policy.
- Some activities on sprint.com that involve collection of user information will trigger a specific notification of how we are going to use that information. An example is when a user signs up for a sweepstakes and provides an email address. Sprint may inform the customer that this email address will be used solely for the purpose of notifying sweepstakes winners. Also, an online notice is provided when a user clicks on a link that navigates outside of Sprint.com to ensure the user is aware that he or she is navigating to a third-party site and that Sprint's privacy policy no longer applies to data a user may provide on the third-party site.

- Some notices are sent directly to the customer. Periodically Sprint will place a notice in the customer's bill and/or send a notice via email, SMS message or direct mail to remind or update them about our privacy policies. One example of this would be the periodic SMS notifications that a Family Locator Services subscriber receives to remind them that they are locatable through that service.
- The use of location-based services such as Sprint Navigation will trigger an on-device notice that informs the customer that the use of this application will require their location information to be collected and used. Another example of on-device noticing is Sprint TV & Movies, which provides an on-device notice and collects consent to access a customer's location information to verify that the content the user is accessing is not subject to blackout restrictions in the user's area.
- On-device noticing is also used to inform our customers of the implications of downloading and using third-party applications. A notice warns the user that when they use a non-Sprint application, Sprint's privacy policy no longer applies. It advises them to check the 3rd party application provider's privacy policy before downloading to determine how their information will be collected and used by that 3rd party provider. These notices can be found at the *Sprint Zone* on smart phones and also are on many feature phones.
- Sprint provides a *Get Started Guide* in our phone boxes. The booklet assists customers with important privacy controls, including passwords protecting their device. On the first page inside the cover there is also an "*Important Privacy Message*" that alerts users to be attentive to privacy considerations when downloading or starting 3rd party applications. This message encourages the customer to check the 3rd party application provider's policies to find out how they will collect, access, use or disclose the customer's personal information.

As you can see from our responses, apart from telecommunications carriers, there are many other parties in the wireless ecosystem that influence or directly collect and use personally identifiable information or location data from wireless handsets, tablets and other mobile devices. This change is directly related to the open platform offered by open mobile operating systems. Today, mobile applications are provided by tens of thousands of market participants who interact directly with consumers. The direct customer relationship with consumers is similar to the model that software, application providers, and websites have had with users of personal computers for decades. The ecosystem involves application providers and developers, mapping agents, handset manufacturers and platform providers, mobile web browsers and search engines, and software developers and providers, as well as carriers. Their services can be assisted by carriers or can be completely independent of the carriers, although the services are enabled by a mobile device.

Examples of location technologies utilized by mobile devices (and applications on mobile devices) that require no carrier involvement include:

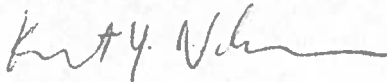
1. End-User Entry (registration for 3rd party applications)

2. Third Party Mapping Services
3. Wi-Fi (Wireless Fidelity)
4. Global Positioning System ("GPS")

Sprint, and the wireless industry in general, strive to be good stewards of users' location information, ensuring that customers understand the uses of location information, have choices, and plainly authorize any disclosure to third parties. With the dizzying array of third party applications now available to users which are not provided by carriers at all, it is understandable that consumers may be confused or less informed. While new third party applications bring many consumer benefits, there are risks too. And because mobile devices now are an open platform, consumers no longer can look to their trusted carrier with whom they have a trusted relationship to answer all of their questions. We appreciate the Committee shining the spotlight on these important issues and hope that third party application providers will take a page from the wireless industry and properly use and protect customer location information.

Your inquiry provides a helpful opportunity to increase transparency, educate consumers about the breadth of the mobile ecosystem, and heighten consumer awareness of ways to protect their privacy on mobile platforms. Thank you for the opportunity to share Sprint's commitment to consumer privacy and education.

Sincerely yours,



Kent Y. Nakamura
Vice President for Policy and Privacy