



Sprint Nextel
900 7th Street, NW
Washington, DC 20001
Office: (202) 585-1902
Fax: (202) 585-1940

Vonya B. McCann
Senior Vice President
Government Affairs
vonya.b.mccann@sprint.com

December 14, 2011

The Honorable Al Franken
Chairman, Subcommittee on Privacy,
Technology and the Law
United States Senate Committee on the Judiciary
Washington, D.C. 20519-6275

Dear Chairman Franken:

Thank you for your letter to Dan Hesse, CEO of Sprint Nextel Corporation (Sprint), dated December 1, 2011, inquiring about Sprint's use of Carrier IQ diagnostic software. Sprint appreciates that your letter reflected both an understanding and acknowledgement of a wireless network operator's legitimate need to deploy and use diagnostic software in the maintenance and operation of its services. Sprint recognizes that it is fair to ask whether the data collected using Carrier IQ software goes beyond "technical diagnostics information", and Sprint's answer is unequivocally no. Sprint takes the privacy of its users and the security of the data it collects seriously so this opportunity to inform the Committee about Sprint's data collection and privacy practices is timely and welcome, especially in light of recent media stories that did not accurately reflect the facts.

As you know, Sprint is a communications company. Sprint is in the business of connecting its customers with their family and friends, getting them online on the mobile web so that they can connect to sites of their choice, and delivering important and life-saving services, such as E911 services and roadside assistance. Sprint is able to deliver these services because it can correctly connect and route customer calls, direct customers' data queries to websites of their choosing, and know how and where to find their devices when they need assistance. Operationally, Sprint knows how to deliver these services on its network. Sprint's customers trust it with the information that it collects and uses in order to deliver communications services to them.

There are some things Sprint does not know. Sprint does not always know why a call drops or a website will not load, for example. Sprint may not always know why a text message is not delivered timely, or why service is unavailable in a particular area. To help it better understand these issues, Sprint uses troubleshooting software installed on customers' devices to report diagnostic and analytics data so it can solve particular problems. Sprint does not need to learn the URL of a website that a user is trying to reach – it is something Sprint already knows from routing the request on its network.¹

¹ Similarly, we know the cell site on which a phone is registering its location, which is necessary for the delivery of voice and data services. We also know the telephone numbers to which our customers have initiated a call or sent a text. Such data is necessary to deliver telecommunications services. In many cases the data collection is required by law and regulations. Under federal law, Customer Proprietary Network Information (CPNI) is also privacy protected. 47 U.S.C. § 222; 47 C.F.R. §§ 64.1200 et. seq.

Discovering, however, why a page did not load requires Sprint to understand what users may be experiencing with their handsets. That is how Sprint has used Carrier IQ -- as a diagnostic tool on devices. The Carrier IQ diagnostic tool can help Sprint engineers understand the functionality (or not) of handset applications when connecting with the network and steps that Sprint might take to improve services and the customer experience, including network enhancements.

Carrier IQ diagnostic software is installed on approximately 26 million Sprint devices. However, the Carrier IQ software tool does not collect any information unless it is "tasked" to do so by Sprint. At any one time, only 1.3 million devices may be tasked to collect and report data. In fact, for any particular research request, a subset of a much smaller number of devices, approximately 30,000, are queried to respond to a research request from Sprint personnel.

Sprint understands that Carrier IQ has shared a technical report with the Committee that describes how the Carrier IQ software works and what data may be available from devices for analysis. The report describes "profiles" that network operators can create for purposes of troubleshooting and understanding network performance. It is important to understand that when Sprint makes a "profile" request to Carrier IQ for certain data, it is not seeking nor does it receive a picture of any particular user's online or mobile behavior over time. To the contrary, a "profile" in Carrier IQ software parlance is a list of analytical data collected from many tasked devices to analyze a certain problem, including conditions or criteria for research of a particular performance issue. For example, a "dropped call profile" could include the signal strength of the cell towers in a particular area for a random volume of calls.

Sprint wants to assure the Committee that data collected by the Carrier IQ tool is transmitted in encrypted form to Carrier IQ and uploaded to the Carrier IQ servers. The data received by Carrier IQ in a raw format is anonymized or otherwise made unreadable by humans before Carrier IQ personnel access or use the data. Carrier IQ analyzes the anonymized data and generally provides Sprint with analytical reports of aggregated metrics based on the anonymized data, thus ensuring that user privacy is not affected in the process. Sprint has not used Carrier IQ diagnostics to profile customer behavior, serve targeted advertising, or for any purpose not specifically related to certifying that a device is able to operate on Sprint's network or otherwise to improve network operations and customer experiences.

Privacy protection is part of Sprint's commitment to customer satisfaction and trust. Sprint implements and follows policies and practices that are transparent and demonstrate its accountability for customer privacy, as well as its compliance with the law. The following responses provide answers to your specific questions.

1. On what devices does your company use or install Carrier IQ software?

Response: Carrier IQ software is installed on a variety of Sprint devices, including mobile handsets and tablets. Various Sprint-offered devices manufactured by the following equipment manufacturers have Carrier IQ software installed: Audiovox, Franklin, HTC, Huawei, Kyocera, LG, Motorola, Novatel, Palmone, Samsung, Sanyo, and Sierra Wireless.

2. As of what date has your company used or installed this software on these devices?

Response: Sprint began including Carrier IQ software on devices in 2006.

3. To the best of your knowledge, how many American consumers use these devices?

Response: To the best of Sprint's knowledge, there are approximately 26 million active Sprint devices that have the Carrier IQ software installed. As noted above, Sprint only "tasks" (queries information about) a fraction of these devices at any one time (a maximum of 1.3 million) for its diagnostic needs; and then only a subset of devices -- approximately 30,000 -- are tasked to research specific problems (e.g., in-network roaming in a given area) with any query.

4. Does your company receive customer location data collected by Carrier IQ software or by Carrier IQ?

Response: Sprint receives information that helps determine the location of "tasked" devices. Sprint uses this information in aggregate to identify and troubleshoot issues occurring in a particular area. However, as a wireless service provider, Sprint knows the location of devices registering on its network irrespective of Carrier IQ diagnostics, and Sprint must know that information in order to route calls and data services, including life-saving E911 services.

5. What other data does your company receive that has been collected by Carrier IQ software or by Carrier IQ?

- a. The telephone numbers users dial?
- b. The telephone numbers of individuals calling a user?
- c. The contents of the text messages users receive?
- d. The contents of the text messages users send?
- e. The contents of the emails they receive?
- f. The contents of the emails users send?
- g. The URLs of the websites that users visit?
- h. The contents of users' online search queries?
- i. The names or contact information from users' address books?
- j. Any other keystroke data?

Response: With the exception of "g" above, Sprint does not receive any of these data elements through the profiles it has established with Carrier IQ. Again, as noted earlier, Sprint already knows the URL of a website that a user is trying to reach from routing the request on its network. This information may be collected through the Carrier IQ software as part of a profile established to troubleshoot website loading latencies or errors experienced by a population of subscribers.

6. If your company receives this data, does it subsequently share it with third parties? With whom does it share this data? What data is shared?

Response: Sprint does not share with third parties Carrier IQ data from customer devices. The Carrier IQ data is used internally for Sprint's own use, for analysis by Sprint employees and contractors to assist with device certification and functionality on its network, and for network maintenance, operation and improvement. In the course of certifying device functionality, prior to selling phones to consumers, Sprint does share and receive certain testing results with handset manufacturers.

7. Has your company disclosed this data to federal or state law enforcement?

Response: Sprint has not disclosed Carrier IQ data to federal or state law enforcement.

8. How long does your company store this data?

Response: Carrier IQ stores data on its servers collected on Sprint's behalf for approximately 30-45 days. Sprint stores raw data received from Carrier IQ for approximately 6 months and stores reports it receives from Carrier IQ based on aggregations of this data for approximately 12 months (data retention may vary depending on the analysis being conducted).

9. How does your company protect this data against hackers and other security threats?

Response: Sprint imposes privacy and security obligations on Carrier IQ through contract with respect to the data housed at Carrier IQ facilities on Sprint's behalf. Such obligations include the use of technical, physical and administrative safeguards and meeting or exceeding industry best practices in safeguarding data. Sprint ensures the security of the reports it receives from Carrier IQ through a series of controls that surround Sprint's IT environment. Sprint uses logical access controls at the operating system, database, and network layers to restrict access to those individuals who have a need-to-know such data. Access at the network layer is terminated when an employee's relationship with Sprint terminates. Database access is reviewed quarterly to ensure compliance with access control policy and procedures. On the periphery, Sprint employs a host of IT security measures including firewalls at all points of entry to Sprint's network, and intrusion detection systems at all Internet points of entry. Sprint has a centralized security department responsible for oversight of security policy, awareness, and enforcement throughout the company. Sprint continuously reassesses its technology and processes to ensure that the security of customer data remains robust and state-of-the-art.

10. Does your company believe that its actions comply with the Electronic Communications Privacy Act, including the pen register statute (18 U.S.C. § 2511 et seq.), and the Stored Communications Act (18 U.S.C. § 2701 et seq.)?

Response: Yes.

11. Does your company believe that its actions comply with the Computer Fraud and Abuse Act (18 U.S.C. § 1030)?

Response: Yes.

12. Does your company believe that its actions comply with your privacy policy?

Response: Yes. Sprint's current privacy policy (sprint.com/legal/privacy) describes the information it collects automatically when a customer uses Sprint services. The policy states in pertinent part:

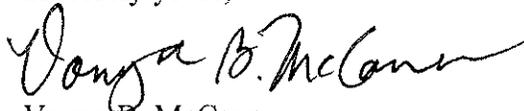
Information we collect when we provide you with Services includes when your wireless device is turned on, how your device is functioning, device signal strength, where it is located, what device you are using, what you have purchased with your device, how you are using it, and what sites you visit. And, Sprint's privacy policy explains that it may use tools and analytics to collect such information.

13. Does it believe that consumers are aware that this activity is actually occurring on their devices?

Response: Sprint believes customers expect service providers and network operators to take reasonable technological steps to maintain the performance of their networks and device functionality in order to effectively deliver call and data services to users. Sprint's privacy policy contains notice of the information we collect, including the notice described above.

Thank you, again, for the opportunity to address Sprint's use of the Carrier IQ tool. As you noted, Sprint has a legitimate need for diagnostic information in providing communications services to its customers. Sprint appreciates and respects the Committee's interest in ensuring that such data collection and use is in full compliance with the law. Sprint trusts that its response makes clear that its use of the Carrier IQ software for such limited purposes is appropriate and that Sprint has followed its privacy policy and all applicable laws.

Sincerely yours,


Vonya B. McCann