

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996;)	CC Docket No. 96-115
)	
Privacy and Security of Information Stored On Mobile Communication Devices)	DA 12-818

COMMENTS OF SPRINT NEXTEL CORPORATION

Vonya B. McCann
Senior Vice President, Government Affairs

Maureen Cooney
Head of Privacy, Office of Privacy

Devin Crock
Counsel, Office of Privacy

Sprint Nextel Corporation
12502 Sunrise Valley Drive
Reston, VA 20196
703-592-7580

July 13, 2012

TABLE OF CONTENTS

I.	INTRODUCTION AND EXECUTIVE SUMMARY	1
II.	A DYNAMIC MOBILE ENVIRONMENT EXISTS	3
III.	BENEFITS OF DIAGNOSTIC DATA COLLECTION TO CARRIERS AND CONSUMERS	6
IV.	PRIVACY AND SECURITY OF INFORMATION ON MOBILE DEVICES - SECTION 222 IS NOT APPLICABLE TO DATA STORED ON THE HANDSETS	9
V.	CONCLUSION.....	14

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996;)	CC Docket No. 96-115
)	
Privacy and Security of Information Stored On Mobile Communication Devices)	DA 12-818

COMMENTS OF SPRINT NEXTEL CORPORATION

Sprint Nextel Corporation (“Sprint”) hereby responds to the Federal Communications Commission’s (“FCC” or “Commission”) public notice seeking comments on the privacy and security of information stored on mobile communications devices.¹

I. INTRODUCTION AND EXECUTIVE SUMMARY

Sprint appreciates the FCC’s inquiry into the security and privacy of customer data on mobile communication devices. The FCC’s leadership role in establishing privacy protections for consumers has strengthened trust between consumers and telecommunications providers and has institutionalized vigilance by carriers in protecting not only the content of communications, but Customer Proprietary Network Information (CPNI).²

It is important to our industry and to consumers that the FCC address carefully the benefits of innovation, evolving mobile business models, new technology, and privacy concerns. Mobile devices have an ever-expanding capacity to serve as ‘smart’

¹ *Public Notice, Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, CC Docket No. 96-115 (May 25, 2012).

² 47 C.F.R. § 64.2001 *et seq.*

information systems while delivering telephone services. The FCC's consideration of privacy practices and risk mitigation should be an iterative process in this rapidly changing area.

Sprint believes that the following points are important for the FCC to take into consideration:

1. There is an evolving and dynamic mobile environment, with new business models and technical functionalities available to and used by consumers. It is appropriate to look both at the benefits of innovation to consumers and also the impact on consumer privacy. Sprint's experience is that current mobile providers address privacy concerns up front by empowering user choice wherever possible. Prescriptive rules are not necessary to meet consumer needs or expectations.
2. The collection of diagnostic data from handsets, in addition to network diagnostic data, is beneficial to our customers and helps carriers provide the services customers expect. Diagnostic information collected by carriers from handsets is generally not the type of data that would identify a particular handset user, would not contain personally identifiable information, and in most circumstances, would not include storage of data that would meet the statutory or regulatory definition of CPNI. Sprint acknowledges that data elements collected by various carriers may differ and their uses of the diagnostic data may differ. But Sprint's data collection has focused on narrowly tailored metrics about specific service performance issues and would not be "customer-specific mobile information" as referenced with concern by the FCC. These metrics or diagnostic data generally involve de-identified data used to produce de-identified and aggregated reports so that we can better understand shared performance issues. These metrics do not involve individual handset or individual user activities, nor are the types of data collected sensitive or particularly impactful on privacy. Sprint is not aware of any incidents of user harm arising from its use of diagnostic tools. Notwithstanding, Sprint's practices have included strong privacy contractual requirements and security of the data metrics while on the phones or in transmission, including encoding the data in a binary, unreadable format to humans while on the handset.
3. Neither Section 222, nor the FCC's CPNI rules apply to data on customer handsets. Requiring carriers to be responsible for the security and privacy of all data on mobile devices would be unworkable and beyond a carriers' capabilities due to lack of carrier design, control, or physical custody of users' devices or insight into what data a particular user may actually have on the users' device. Carriers are no longer the gatekeepers of the mobile experience. In an open environment, both as to platform design, phone design, and the ability of users to configure their phones and uses of mobile devices, this is especially true.

4. Sprint believes that transparency of data practices by carriers is a key privacy tenet, and we strive to inform our customers of our practices. Transparency allows consumers to assess a carrier or other ecosystem stakeholder's practices and to make decisions about choosing to engage with the service provider or on how to tailor their use of services provided. Sprint tells customers about the data that we collect and in our privacy policy explains our data practices. In addition, Sprint strives to develop broader means of communicating clearly with customers, including finding new ways to inform users with on-device notices and introducing privacy controls.

There is an important role for carriers, other members of the mobile ecosystem, and the FCC to play in advancing privacy and data security. Consumers should be educated on the tools and information available to protect identifiable and sensitive data on their phones and carriers should continue to protect privacy in an evolving market. Using the CPNI framework to address confidentiality of all data, however, is not appropriate.

II. A DYNAMIC MOBILE ENVIRONMENT EXISTS

Since the FCC's inquiry in 2007, the use of smart phones by consumers has proliferated dramatically, causing a sea change in the mobile environment. In addition to using mobile communications devices for telephone services, consumers are taking full advantage of their mobile devices to connect to the Internet, send e-mail and text messages, download applications, and use media features provided on or through their smart phones, including access to television, camera and video capabilities.

The mobile device can be the platform through which consumers shop, bank, organize their schedules and contacts, and it may be the primary tool used as an education platform or to receive news or network with friends online. New uses of mobile devices transform the ways individuals interact with and depend upon health professionals and services, receive advertising and discount promotions, or connect with government

institutions, as well as libraries and non-profits not only in their home towns, but around the world.

The ability of mobile devices to process and store data efficiently also has expanded. Carriers strive to keep up with this demand by enhancing our networks and their ability to facilitate both voice and data services used to better meet customer expectations.

To meet these demands, consumers expect that carriers will seek to understand the interactions between the vast array of mobile devices and the carriers' networks in an effort to improve performance and provide reliable basic and enhanced services. Indeed, mobile devices are an integral part of wireless operations – the performance of devices affects the performance of the network and the customer experience. As a result, collecting diagnostic information about the interface between these various devices and a carrier's network can be key to understanding performance issues and providing better services to consumers.

Sprint's experience is that consumers expect service quality to be 'baked in' through design, testing, monitoring and by pushing software updates, sharing tips for using mobile devices, and building network enhancements to correct or improve functionality. This is the identical activity users experience through their wired devices as software makers push updates automatically and wire line access providers similarly monitor device connection and usage on their networks.

While new functionalities and uses by consumers of 'smart' mobile devices require carriers to be 'smarter' in understanding and delivering connectivity and enabling a variety of basic and enhanced services, carriers have been addressing emerging privacy impacts of these new functionalities. The absence of law or regulation, or the lack of

applicability of specific statutory privacy provisions to particular data collection and uses, has not been an impediment to carriers implementing privacy protections that protect their customers.

Key examples of these efforts, as pointed out in the FCC's report on Location Based Services and location privacy, include the development and commitment by carriers to adhere to CTIA Guidelines and Best Practices on Location Based Services, outreach to app developers on application privacy, providing notices to users and guidance on issues ranging from awareness about protection of data collected through applications by third parties, to tools and tips on securing and safeguarding data stored by users on their phones and how to adjust privacy settings. Carriers themselves also build in privacy by design in their contractual relationships with vendors and third parties concerning privacy and security protections around data collection and use.

Privacy by design is sensible for carriers to consider with any data collection, regardless of statutory or regulatory mandates if they are focused on customer satisfaction. Privacy by design considerations should include considerations about limitations on data collection and types of data collected, transparent disclosure of the use of diagnostic tools, appropriate security protocols around data on the handset and in transmission, appropriate contractual privacy provisions with vendors and handset manufacturers, and tailored requests for samples of diagnostic data for specific uses, the format of reports on diagnostic data – such as in a de-identified and aggregated format, access controls to data, and proper retention and storage requirements.

III. BENEFITS OF DIAGNOSTICS DATA COLLECTION TO CARRIERS AND CONSUMERS

A. Carriers Have a Need to Understand Performance Issues from the “Handset’s Perspective” in Addition to a Network Perspective

Carriers are able to make assessments about their network performance by monitoring their networks. However, there are aspects of customer experiences and assessment of actual service events that cannot be measured or understood without collecting particularized data from a sampling of handsets, for instance handset on-network and off-network performance at particular locations or times. Handset data is critical to maintaining and operating a carrier’s network because a carrier cannot understand the device experience during a particular event, such as a dropped call, by simply monitoring its network alone. To assist in determining whether problems experienced by customers are due to network issues or handset issues, such diagnostics are essential and permitted by law.³

Remote diagnostic data largely is made up of device and network identifiers (e.g. tower or base station IDs), operating data (e.g., signal strength), and event data (e.g., the initiation of a function and whether it was completed, whether a call was abandoned or dropped). The data collected does not provide a picture of the customer’s mobile or online behavior, particularly if deployed in a manner that does not readily identify a customer with a device and if the diagnostic survey is periodic, rather than continuous, and data elements are collected in a tailored fashion on specific performance issues. Of course, as a wireless Internet access provider, customer usage is readily apparent and available to the provider and subject to privacy and security protections that already exist under the law and industry best practices. Diagnostic tools do nothing more than assist

³ 47 U.S.C. § 222(d)(1).

the provider to better understand performance issues by aggregating data and incorporating handset information like signal strength, for example.

Sprint's general experience in the use of diagnostics data collection from handsets, as reported previously, has not been customer-specific; rather, Sprint has developed and used reports of de-identified device information and aggregated data to understand group performance situations and design solutions for network enhancements.⁴ This is not sensitive or personal information collected on the handset and it is generally not CPNI-related. What Sprint has learned from sampling a pool of diagnostic metrics from devices in particular locations or with particular problems at set times is that we are collecting data that may be relevant not to a single customer, but across our customer base. Sprint has used such data metrics to pinpoint and understand performance challenges, design solutions, and work with handset manufacturers on a particular issue or identify where we might need to enhance Sprint's network planning. These efforts both assist carrier understanding of how to deliver services in an environment of greater demands for efficiency and assist consumers in receiving the services that they expect when they use their mobile devices.

B. Through Privacy Policies and Other Channels Carriers Inform Consumers on Data Collection Practices

In Sprint's experience, disclosure of data collection is provided through a variety of channels, including through privacy policies, terms and conditions, online, and in device settings, alerts and other consumer communication vehicles. Sprint provides notice to consumers about diagnostics data collection in its privacy policy and other

⁴ Letter from Vonya B. McCann, Senior Vice President, Government Affairs, Sprint Nextel Corporation, to the Honorable Al Franken, United States Senate (Dec. 14, 2011).

communication vehicles, such as the Frequently Asked Questions on its privacy page (available at sprint.com/privacy). For example, Sprint’s privacy policy states that:

“We automatically receive certain types of information whenever you use our Services...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...”

Our privacy policy goes on to state that Sprint uses such information to “[m]onitor, evaluate, or improve our Services, systems, or networks.” Sprint is committed to providing our customers with the best possible mobile experience, connecting our customers with their family and friends, and getting them online, and delivering quality mobile services. To do so, Sprint needs to know how best to connect and route customers calls, direct customers’ data queries to websites of their choosing, and locate their devices. Sprint can best provide these services by understanding how our customers’ devices interact with our network, working constantly to improve the customer experience.

On its Privacy FAQs page,⁵ Sprint states that it may collect information from devices and that it “may use diagnostic tools, including on-device aids for this purpose to improve the quality of service and network performance for our customers.” To better understand why devices may not function properly, Sprint needs to collect information from devices. Sprint believes its customers expect service providers and network operators to take reasonable technological steps to maintain the performance of their networks and device functionality to provide robust and efficient services to consumers.

In addition to carrier disclosures and use of diagnostics, as the Commission is aware, diagnostic analytics may be collected from handsets by manufacturers, platform

⁵ Available at www.sprint.com/privacy.

providers and application providers. Carriers are no longer the gatekeepers or sole enablers of the mobile experience. Many players have a role in a user's mobile experience, from platform providers to device manufacturers to application providers, as well as carriers. The FCC's focus on carrier collection, and even on the applicability of Section 222 protections, does not address the wider ecosystem of players in the current mobile environment.

IV. PRIVACY AND SECURITY OF INFORMATION ON MOBILE DEVICES – SECTION 222 IS NOT APPLICABLE TO DATA STORED ON HANDSETS

Customer information on mobile devices is subject to a myriad of protections, whether implemented by carriers or chosen by consumers. Sprint is committed to ensuring that any data it collects from devices is protected on the device as well as in transit back to Sprint. Additionally, the mobile industry continues to provide robust applications and services to ensure consumers may choose security measures based on the data they store on their devices, convenience of access, and other concerns.

A. Remote Diagnostic Data is Protected While on Mobile Devices

Sprint protects remote diagnostic data collected from customer devices through the same contractual, administrative, technical, and physical protections with which Sprint protects all customer data. Remote diagnostic data on a device generally is placed in portions of the device that are not readily accessible. Further, such data is encoded while on the device and, therefore, not in a form readable by humans even if accessed.

Remote diagnostic data uploaded to Sprint's network is protected by the same means by which Sprint protects our mobile network. Remote diagnostic data is protected and encrypted on Sprint's CDMA network when sent to collection servers housed behind Sprint's firewall. The data is sent via dedicated paths to analytics servers for aggregation

into reports. This ensures that remote diagnostic data has been protected from creation through the analytics process.

B. Consumers Are in the Best Position to Choose the Security Measures for Their Mobile Devices

Mobile devices are no longer the exclusive domain of wireless carriers. Since 2007, consumer adoption of smart phones has increased dramatically. This transition from feature phones has coincided with a change in the role of carriers with respect to mobile devices; carriers are no longer gatekeepers of mobile devices. Many different entities have a significant role in the development, production and offering of mobile devices. Such entities include device and operating system manufacturers, social media companies, application developers and service providers.

The wireless industry is providing consumers various ways in which to enhance the privacy and security of their devices, and it is Sprint's goal to encourage customers to take advantage of the tools available to them. For example, we encourage our customers to protect their devices and services with strong passwords.⁶ Additionally, we strive to educate our customers about products and services they can use to tailor their devices and services with effective mobile security tools.

In 2011, Sprint partnered with McAfee to provide our customers with easy access to McAfee Mobile Security and McAfee Family Protection Android Edition software, which helps to protect information stored on mobile devices. The software provides various tools to protect mobile devices such as the ability to locate lost or stolen devices, remotely lock and wipe mobile devices, and malware protection.⁷ Through our Sprint

⁶ See Sprint's Privacy FAQs available at www.sprint.com/privacy.

⁷ Sprint also is a participant with other carriers in the Stolen Handset Initiative to thwart cellphone and tablet theft and threats to users from criminal elements because of access to user personal information and sensitive data.

Zone application and online, we have recommended other mobile security applications such as the Norton Mobile Security and Lookout Security apps. Further, Sprint launched a Mobile Security Council, along with partners like McAfee and Lookout, to jointly assess emerging security issues and provide timely solutions to consumers.

The mobile industry is committed to providing customized solutions to meet consumers growing needs. Some smart phones now come with multiple methods of locking the device – PIN codes, pattern codes, and even facial recognition. Voicemail clients can be protected by PIN codes, and there are other applications available that place locks on other applications on the device. A quick search on any of the available app stores for “security” will bring up a myriad of services designed to protect customer information on their mobile devices. Similar to the customization that exists in an open mobile environment, consumers have many means with which to protect the data on their mobile devices. With these tools, consumers are in the best position to choose the security methods that best meet their needs.

C. Remote Diagnostic Data and Information Stored on Mobile Devices by Consumers is Not CPNI

CPNI⁸ is a statutorily defined term and in order for data to be CPNI it must (1) relate to the quantity, technical configuration, type, destination, location, or amount of use of a telecommunications service; (2) relate to service subscribed to by a specific customer; and (3) be made available to the carrier by the customer solely by virtue of the carrier-customer relationship.⁹ CPNI does not encompass all data made available to carriers through the customer-carrier relationship; rather, the information must relate to

⁸ 47 U.S.C. §222(h) (1).

⁹ Sprint notes that there are other types of CPNI, specifically information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. *Id.*

the categories of data outlined in the statutory definition. Neither remote diagnostic data collected by carriers, nor information stored by customers on their devices meets the definition of CPNI.

Remote diagnostic information is not CPNI, because it does not relate to the quantity, technical configuration, type, destination, location, or amount of use of a telecommunications service subscribed to by a customer. Remote diagnostic data does not provide details on a customer's mobile usage, rather the data provides a look at the performance of carrier networks and a consumer's mobile device during certain events such as dropped calls.

Remote diagnostic data can generally be categorized as device and network identifiers (e.g., tower or base station IDs), operating data (e.g., signal strength), and event data (e.g., whether a call was abandoned or dropped). None of these data elements provide information on the quantity, technical configuration, type, destination, location, or amount of use of a telecommunications services subscribed to by a consumer. The data is the information carriers typically collect over their networks to understand network performance; remote diagnostic data simply provides the same understanding from a handset perspective. The data do not provide a picture of any particular user's online or mobile behavior over time.

In addition, the data collected from devices is usually device specific, and not consumer specific. Meaning, the information is collected about how a device functioned and is not linked to individual users. Carriers use this information to develop aggregate-level reports on how devices interact with their networks. The purpose of remote diagnostic data collection is not to analyze individual consumers' usage, and the reports

generated by carriers could not be used to create a detailed picture of a specific customer's usage.

In its Public Notice, the FCC asked whether data on a device at the direction of carriers could be considered CPNI even before it is transmitted to the carrier. Because the remote diagnostic data does not relate to the categories of data that make up CPNI and the data is not customer specific, remote diagnostic data is not CPNI while on the device or when collected by carriers.

D. Consumer Information Stored on Devices is Not CPNI

As mobile devices become more dynamic, open, and powerful, the potential uses for consumer devices increases, which in turn means that there is a nearly endless set of possibilities of "customer data" that could be stored on a device. As stated above, consumers are using their mobile devices as media platforms, mobile work stations, and organizers for all manner of personal data. However, consumer information stored on mobile devices is not CPNI and not subject to carriers' obligations under Section 222.

First, most information stored by customers on their devices is not made available to carriers. With the proliferation of smart phones and downloadable apps, there are an endless number of companies that can connect with customers through their mobile devices. While certain companies can collect data about customers through use of apps, the data is not generally available to carriers. Carriers may have access to certain data on devices; e.g., the remote diagnostic data discussed above; but carriers do not collect all data stored on a device.

Second, customer information stored on the device rarely pertains to the quantity, technical configuration, type, destination, location, or amount of use of a telecommunications service. Generally speaking, most of the data on the device is either

entered into the device by consumers or generated through a consumer's interaction with a mobile app. The former could be any type of data the customer chooses to enter – such as contact names and phone numbers or a grocery list. The latter are provided generally via a mobile broadband app and do not relate to a customer's use of a telecommunications service. Moreover, the data is not generally available to the carriers via the customer-carrier relationship. Thus, the data does not meet the definition of CPNI.

We note that, in any case, Section 222 plainly contemplates that carriers may access and use CPNI on an individualized basis for many purposes, such as with the user's consent, to initiate, render, bill, and collect for telecommunications services; to protect the rights or property of the carrier; or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

Further, the Stored Communications Act, which applies equally to data collected by a carrier, permits such access and use to render any service, and a myriad of applicable state laws permit such access for the maintenance of the network and its repair and operation. The FCC must consider the entire legal framework applicable to data to avoid creating inconsistent or redundant rules or introducing confusion into the marketplace.

V. CONCLUSION

Sprint appreciates the FCC's effort to revisit the issue of privacy and security of information stored on mobile devices. The mobile ecosystem is a fast changing environment and it is important to review and update the record periodically. Privacy and security protections for mobile devices have continued to evolve along with the rest of the mobile products and services available to consumers.

While there certainly could be sensitive information stored on a device, sweeping all consumer data stored on a device under the protective rug of Section 222 is improper

and unnecessary. Consumer data stored on devices is not CPNI for the reasons stated above. Further, the mobile industry provides consumers with a number of choices to protect their mobile devices and the information stored within making such a regulatory catch-all unnecessary.

Respectfully submitted,

SPRINT NEXTEL CORPORATION

/s/ Vonya B. McCann _____
Vonya B. McCann
Senior Vice President, Government Affairs

Maureen Cooney
Head of Privacy, Office of Privacy

Devin Crock
Counsel, Office of Privacy

Sprint Nextel Corporation
12502 Sunrise Valley Drive
Reston, VA 20196
703-592-7580

July 13, 2012