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

May 23, 2012

The Honorable Edward J. Markey
Co-Chairman
Congressional Bi-partisan Privacy Caucus
2108 Rayburn House Office Building
Washington, DC 20515-2107

Dear Representative Markey:

Thank you for your May 2, 2012, letter to Dan Hesse, CEO of Sprint Nextel Corporation ("Sprint"). Sprint welcomes the opportunity to address a number of fictions and mischaracterizations circulating in the press and elsewhere regarding wireless carriers' provision of customer information to law enforcement. Any suggestion that Sprint is cooperating with law enforcement in an inappropriate manner is seriously misplaced.

Sprint complies with all applicable laws. When responding to law enforcement, if Sprint does not receive a valid legal demand or other appropriate document[1] that is suitable for release of the specific information being sought, Sprint will not disclose customer information. Sprint takes these obligations seriously and recognizes both the obligation to comply with legal demands and the obligation to protect our customers' information.

STATUTORY BACKGROUND

By way of background it may be useful to review the federal statutes that prohibit Sprint from voluntarily disclosing customer data to law enforcement.[2] In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA") in response to concerns that the Fourth Amendment did not apply to data stored by third parties. By amending federal statutes relating to usage of wiretaps and pen register/trap and trace devices, and by creating new statutory authority to protect stored communications, Congress created statutory privacy rights for customers of Sprint and other communication service providers.

---

[1] We refer throughout to a legal "demand" because that is exactly what it is – a legal obligation. Nonetheless, there are circumstances, which are outlined in the applicable statutes, where information can be disclosed to law enforcement with the consent of the customer or in certain emergency situations. In those cases, Sprint still requires appropriate documentation, and although it may not be a legal demand, *per se*, it is legally permissible for Sprint to provide the information under the statute, as discussed herein.

[2] Of course there are numerous state statutes that also require that Sprint release customer information to law enforcement but, because no state statute can require less than the federal statutes, it is appropriate to focus on the federal laws.

Today, the ECPA is comprised of three statutes: the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, the Pen Register and Trap and Trace Devices Act ("PR/TT Act"), 18 U.S.C. § 3121, *et seq.*, and the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.* Together these statutes provide different levels of protection for customer records and information from disclosure to the government. Appropriately, the more customers' privacy rights are implicated, the more stringent the requirement for the government agency seeking disclosure:

(1) Basic subscriber information, which is strictly limited to six specific categories of information (name, address, local/long distance records (or records of session times and duration), length/type of service, telephone/subscriber number and means and source of payment), is the only information that can be disclosed to law enforcement pursuant to an administrative, grand jury or trial subpoena. 18 U.S.C. § 2703(c)(2).

(2) All non-content records or other information pertaining to a subscriber (including basic subscriber information) can be disclosed to law enforcement pursuant to a court order based on "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

(3) The stored content of a customer's communications (*e.g.*, text messages), can only be disclosed to law enforcement pursuant to a warrant or court order based on probable cause. 18 U.S.C. §§ 2703(a) & (b).

(4) A wiretap can only be established pursuant to a court order based on probable cause. 18 U.S.C. § 2702(b)(2) & 18 U.S.C. § 2518(3).

Importantly, each of these demands for customer information has repercussions for Sprint if it fails to provide the requested information. If Sprint fails to comply with a subpoena for basic subscriber information, the government can seek to compel its production via a court order and can impose costs and other fines on Sprint. If Sprint fails to comply with a valid court order, the company can be found in contempt of court and subject to fines and other penalties. Moreover, if Sprint fails in its obligations to abide by the ECPA, the company can face civil penalties for violation of the statute. 18 U.S.C. § 2707. When Sprint responds to demands from law enforcement, it is not cooperating in some surreptitious fashion but instead is complying with the law that Congress established to permit disclosures of our customers' information to law enforcement under certain limited circumstance.

LOCATION INFORMATION

Much of the reporting in the press relates to how law enforcement personnel obtain location information from wireless telecommunications carriers. This is an evolving area of law and one which Sprint believes requires further clarification by Congress.

To understand this issue fully, one must understand what types of information and capabilities wireless carriers have with respect to the location of a mobile device. First, Sprint has business records that contain information on the location of a wireless device based on that device's proximity to nearby cell towers. The information in Sprint's records is often referred to as "historic" or "stored" location as it is customer information of a historic nature that is stored by Sprint for its own business purposes. For

example, Sprint uses this type of information for certain billing, taxing, network troubleshooting and capacity planning purposes. Sprint also has the capability to determine the location of a cell phone in real time by using GPS technology.[3]

The location information contained in Sprint's business records is not basic subscriber information as defined by the statute but is information Sprint has relating to its customers' mobile device usage. Consequently, a court order based on "specific and articulable facts" is required prior to disclosure of that information to law enforcement. 18 U.S.C. § 2703(d). There are some jurisdictions, however, where courts have determined that a warrant based on probable cause is required for release of this type of historic or stored location information and, as a result, in those jurisdictions the higher standard for a warrant, *i.e.*, probable cause, must be met before disclosure of historic location information to law enforcement. *In re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010)

There is no statute that directly addresses the provision of location data of a mobile device to the government. While the Communications Assistance for Law Enforcement Act ("CALEA") prohibits the provision of location information in conjunction with a pen register or trap and trace device (*see*, 47 U.S.C. § 1002 (a)(2)(B)), the D.C. Circuit Court of Appeals found that location information could be "call-identifying information" under CALEA and therefore a service provider must deliver it to law enforcement when authorized. *USTA v. FCC*, 227 F.3d 450 (D.C. Cir. 2000). The Department of Justice has taken the position that a combined PR/TT and Section 2703(d) order based on "specific and articulable facts" authorizes a wireless carrier to deliver (i) single cell site at the start or end of a call; (ii) all cell sites serving a call for triangulation; (iii) all registration information; and (iv) location of associates on a call with the target. A number of federal magistrate judges, however, have rejected the DOJ position, concluding that the use of a cell phone as a tracking device requires probable cause and a search warrant under 18 U.S.C. § 3117. *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp.2d 747 (S.D. Tex. Oct. 14, 2005); *In re Application of the United States for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device*, 396 F. Supp.2d 294 (E.D.N.Y. Oct. 24, 2005); *see also Justice Dept. Defends Warrantless Cell Phone Tracking*, Declan McCullagh, Feb. 13, 2010, http://news.cnet.com/8301-13578_3-10453214-38.html; *and Location, Location, Location: Three Recent Court Controversies on Cell Phone and GPS Tracking*, Kevin Bankston, Dec. 1, 2010, http://www.linuxbsdos.com/2010/12/01/location-location-location-three-recent-court-controversies-on-cell-phone-gps-tracking. And, in January, the Supreme Court clarified in *United States v. Jones*, that a warrant was required before law enforcement could use a tracking device attached to a car but specifically left open the question of whether tracking the location of a mobile device might be subject to the same privacy protections. *United States v. Jones*, 132 S. Ct. 945 (2012) (Alito, concurring). Moreover, there is an argument that a mobile device could meet the definition of a tracking device under 18 U.S.C. § 3117.

Given the importance of this issue and the competing and at times contradictory legal standards, Sprint believes that Congress should clarify the legal requirements for disclosure of all types of location information to law enforcement personnel.

[3] The FCC requires that wireless carriers have the capability to locate a wireless caller for 9-1-1 purposes. The level of accuracy that must be provided depends upon the capability of the Public Safety Access Point ("PSAP") receiving the call. The accuracy rules for wireless 911 calls are set forth in 47 C.F.R. 20.18(h).

RESPONSES TO YOUR SPECIFIC QUESTIONS

1. *How many requests has Sprint received from law enforcement over the past five years and how did the company respond to each?*

Over the past five years, Sprint has received approximately 52,029 court orders for wiretaps; 77,519 court orders for installation of a pen register/trap and trace device; and 196,434 court orders for location information. These court orders were issued by a variety of federal and state courts at the request of hundreds of different federal and state law enforcement agencies. Over this same time frame, Sprint received subpoenas from law enforcement agencies requesting basic subscriber information. Each subpoena typically requested subscriber information on multiple subscribers and last year alone we estimate that Sprint received approximately 500,000 subpoenas from law enforcement. Determining how Sprint responded to each of these legal demands would require a manual process of reviewing each demand and what was provided in response – an objection, a rejection, information, etc. – and comparing that response with what was originally requested by the law enforcement agency. Unfortunately, Sprint does not have the resources to research each of these many legal demands.

2. *How much staff is devoted to providing information to law enforcement and what protocols and procedures do they employ?*

Pursuant to the legal requirements of CALEA, Sprint is required to have a team available 24 hours per day, 7 days per week to respond to demands from law enforcement. 47 C.F.R. §§ 64.2100 *et seq.* (implementing 47 U.S.C. § 1006). As a result, Sprint employs a team of 36 analysts who receive court orders for location and installation of wiretaps and pen register/trap and trace devices. This team is responsible for reviewing the language of the order to ensure that the order supports the requested information and then for ensuring that the order is fulfilled appropriately. In addition to this group, Sprint employs approximately 175 additional analysts to respond to subpoenas and court orders for subscriber information that the company receives from both civil litigants and law enforcement. All of these analysts are supported by 10 managers and supervisors.

This entire team of personnel receives regular training on the laws applicable to law enforcement demands for information and meets routinely with legal counsel to review any issues or concerns regarding court orders or other legal demands that the company receives. Typically, if one of Sprint's analysts believes a court order or subpoena is insufficient, that analyst will send a letter back to the requestor explaining why the requested information cannot be provided. Often, the requestor will respond with an explanation of why, in their view, the order provides sufficient authority to obtain the requested information. These discussions can result to an escalation to in-house counsel at Sprint who discusses the issues with the Assistant US Attorney or state attorney and can result in further escalation to Sprint's outside legal counsel to become involved before the court if it is necessary to seek withdrawal of the order or move to quash it.

3. *How does Sprint handle emergency requests for tracking?*

Sprint has specific processes that it employs when an emergency request for information is received without an appropriate legal demand. For example, Section 2702(c)(4) of the SCA permits Sprint to comply with law enforcement requests in emergency situations when Sprint believes there is an emergency involving danger of imminent death or serious physical injury. In those circumstances, our processes require law enforcement to fax in a form which we use to authenticate the law enforcement requestor and to help verify that an appropriate emergency exists. After being satisfied that the statutory requirements have been met, the Sprint analyst will comply with the request but only for 48 hours,

providing law enforcement with sufficient time to obtain appropriate legal process. To be clear, in these particular circumstances, providing information to law enforcement is not required and Sprint could decide that it will not comply with these emergency requests. Sprint has determined, though, that on balance it is in the interest of our customers and members of the general public who may be at risk to comply with emergency requests, particularly since they often involve very serious life-threatening situations such as kidnapping, child abduction and carjacking. When Sprint analysts have any questions concerning the authority to respond to a law enforcement request under these emergency circumstances, they are required to contact internal Sprint counsel before responding and routinely do so.

4. *Has Sprint encountered misuse of cell phone tracking by law enforcement or law enforcement personnel using their own tracking equipment?*

As described herein, Sprint takes its obligations seriously in responding to law enforcement demands and only responds when it receives a demand appropriate for the information being requested. Sprint is not aware of incidents of misuse of cell phone tracking by law enforcement and does not keep records of such information. Similarly, Sprint is not aware of law enforcement personnel using their own tracking equipment and does not cooperate with law enforcement involved in any such activities.

5. *Has Sprint accepted compensation in exchange for providing information to law enforcement?*

Law enforcement is required by statute to compensate carriers for the expenses incurred in responding to law enforcement demands.[4] Section 2518(4) of the Wiretap Act requires that providers be compensated "for reasonable expenses incurred in providing such facilities or assistance" to accomplish any court-ordered interception or wiretap. Section 3124(c) of the PR/TT Act likewise requires that providers be "reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance" for the installation of a pen register or trap and trace device. And, Section 2706 of the SCA requires that the government pay "such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing [the contents of communications, records, or other information]." Moreover, the court orders that Sprint receives routinely contain language requiring law enforcement agencies to compensate Sprint for any assistance in complying with the request. While there are no state or federal laws, rules or cases defining what constitutes "reasonable" expenses in these contexts, Sprint only seeks reimbursement for the costs and expenses it incurs from responding to law enforcement demands. Sprint established rates based on our actual costs of responding to demands from law enforcement personnel and believes it fair and reasonable to inform law enforcement of what those rates are by providing them with a fee schedule. Sprint's current fee schedule, which has been in effect since August 2010, is attached for your review. Sprint does not seek to profit from responding to law enforcement demands and it does not charge law enforcement in connection with emergency requests.

6. *Does Sprint actively market the provision of information to law enforcement?*

Sprint does not market the provision of information to law enforcement. As described herein, Sprint is required by laws passed by Congress to respond to legitimate demands from law enforcement for our customers' records and information. Sprint also is required to file its policies and procedures for compliance with CALEA with the Federal Communications Commission. 47 CFR ¶ 1.20005. Moreover,

[4] There is an exception to this requirement. Law enforcement need not compensate carriers for the provision of "records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings" except if the court determines that provision of such information is "unusually burdensome." 18 U.S.C. § 2706(c).

Sprint provides law enforcement with its policies and procedures so they have information on how to contact Sprint for processing of their legal demands. As stated above, Sprint also provides a fee schedule to law enforcement so that they are informed about the rates they will be charged by Sprint for responding to their legal demands. Sprint is not marketing these services, but providing appropriate information to law enforcement consistent with our legal obligations and duties.

* * *

I hope this letter explains Sprint's obligations to respond to law enforcement demands and fully answers your questions regarding our practices. As described herein, the law is quite clear on the duties and obligations Sprint has in responding to law enforcement demands for customer information except with respect to the provision of location information to the government. The absence of a clear statutory framework regarding the legal requirements for provision of location information to the government and ambiguity arising from the evolving case law suggest Congress should clarify the law to provide certainty for all stakeholders. If Sprint can be of further assistance to you in this regard, please let me know.

Very truly yours

Vonya B. McCann

Attachment

cc: Charlie R. Wunsch

Electronic Surveillance Fee Schedule		
Type of Request	Fee	Notes
- Pen Register Trap & Trace (PRTT) - Wiretaps *Note: A PRTT is a single data channel. A wiretap is a single data & content channel.*	1) Implementation fee per each voice or Push-to-Talk (PTT) intercept: - $342.11 2) Daily maintenance per each voice or PTT intercept: - $10 (this includes 2nd set of IDs & PWs) *NOTE: Other technologies like femtocell, 3G, 4G, or text messaging are included in above rate unless provisioned without voice or PTT*	- Implementation fee is a flat rate. - Daily maintenance covers all electronic surveillance maintenance on intercepts including upgrades, number changes, extensions, etc. - Exigent intercepts are free of charge until Sprint receives a court order.
Late extension to intercept (LEA sends CALEA request after prior surveillance has expired)	Applicable implementation fee.	Daily maintenance applies.
Precision Location	- Manual requests are $20 for each time we provide location per #. - L-Site is unlimited requests for $30 a month per #. *NOTE: No fee in exigent, PSAP, or customer consent situations.*	Provides real-time precise location information on mobile device.
- Electronic Communications in Storage (ECS) - Contemporaneous Billing - Cell site / sector	$30 per case hour worked. Minimum of 1 hour per case plus $7.50 for each 15 minutes worked. *NOTE: No fee in Exigent, PSAP, or customer consent situation.*	- Stored Includes text messages, voice mail retrieval, stored photo/video, historical e-mail. - Cell site / sector provide real-time cell site / sector of requested #.
Account Takeover	$300 per target account plus any accrued charges on subject account	LEA takes responsibility for any billed amount on subject account. Keeps account from being suspended for non-payment. Not always 100% effective & may not be transparent to subject.