



**Sprint Nextel**  
Suite 700  
900 7th Street, NW  
Washington, DC 20001  
Office: (703) 433-3786  
Fax: (202) 585-1940



**Charles W. McKee**  
Vice President - Government Affairs  
Federal and State Regulatory  
charles.w.mckee@sprint.com

October 3, 2013

The Honorable Edward J. Markey  
United States Senate  
218 Russell Senate Office Building  
Washington, DC 20510-2107

Dear Senator Markey:

Thank you for your September 12, 2013, letter to Dan Hesse, CEO of Sprint Corporation ("Sprint"). Sprint welcomes the opportunity to provide you additional information about the circumstances under which wireless carriers provide customer information to law enforcement. Sprint takes seriously its dual responsibilities of responding to lawful inquiries while at the same time safeguarding our customers' privacy.

In response to your letter last year, Sprint provided detailed background information about the various statutes governing Sprint's responsibilities to provide information to law enforcement. In addition, Sprint described its procedures for collecting customer information and the limits of its capabilities. Because there have been no material changes in either the law or Sprint's processes in the last year, Sprint does not repeat that background information here. However, the legal uncertainty in this area has not changed, and Sprint again urges Congress to clarify the legal requirements regarding the disclosure of location information to law enforcement personnel. Competing and at times contradictory legal standards often govern this important issue.

### **RESPONSES TO YOUR SPECIFIC QUESTIONS**

1. *In 2012, how many total requests did you company receive from law enforcement to provide information about your customers' phone usage?*
  - a. *Within that total, please list the amount of requests your company received for each type of usage, including but not limited to the following: 1) Geolocation of device (please distinguish between historical and real-time; 2) Call detail records (i.e. pen register and trap and trace); 3) Text message content; 4) Voicemail; 5) Cell tower dumps; 6) Wiretapping; 7) Subscriber information; 8) Data requests (e.g., Information on URLs visited).*
  - b. *Within that total, how many of the requests were made in emergency circumstances and how many were in non-emergency situations?*
  - c. *Within that total, how many of the requests did your company fulfill and how many did it deny? If it denied any requests, for what reasons did it issue those denials?*
  - d. *Within that total, please breakdown how many of the requests were made by Federal authorities, how many by state authorities, and how many by local authorities.*

Sprint has a database system that processes the intake and distribution of law enforcement requests, such as those listed above, to a team of analysts for response. The primary function of

this system is to allocate work and monitor employee performance in responding to law enforcement requests. Sprint's systems, however, do not track the number or types of requests using the categories listed above in a manner that makes it possible for Sprint to provide the detailed information requested in your question.

In reviewing the publication of the wireless carriers' responses to your data requests last year, it is apparent that there are no uniform standards by which the various carriers catalog these requests, and the responses to your inquiry varied widely. For example, is a subpoena seeking information on more than one telephone number considered a single request or multiple requests? If an order is issued that extends a current wiretap, is that a second request or should it be discounted because a previous request had been issued?

Rather than attempting to provide numbers that are not comparable with other carriers, Sprint would be happy to meet with you and your staff in person to discuss the number of requests and the manner in which they are retained.

2. *For each type of usage in 1(a), how long does your company retain the records?*

Sprint's standard retention period for law enforcement requests is 18 months.

3. *What is the average amount of time law enforcement requests for one cell tower dump (e.g., one hour, 90 minutes, two hours, etc.)? For each hour of a cell tower dump that your company provides, on average how many mobile device numbers are turned over to law enforcement?*

Sprint receives requests for "tower dumps" from federal, state, and local law enforcement agencies. Sprint does not track the average duration of each dump nor the average number of mobile device numbers that are provided to law enforcement in response to each such request.

4. *In 2012, how many requests did your company receive under Section 215 of the Patriot Act?*

Section 215 of the Patriot Act, codified at 50 U.S.C. § 501 *et seq.*, prohibits Sprint from disclosing "to any other person ... that the Federal Bureau of Investigation has sought or obtained tangible things under this section." *Id.* § 501(d). Sprint, therefore, cannot provide any information about requests under Section 215, including whether or not Sprint has received such a request.

5. *What protocol or procedure does your company employ when receiving these requests?*

- a. *What legal standard do you require law enforcement to meet for each type of usage in 1(a)?*
- b. *Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency tracking requests? If yes, what are the distinctions?*
- c. *Have any of these practices changed since your May 2012 correspondence?*

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 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 retains 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 managers and supervisors.

This entire team 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 a Sprint analyst 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 in an escalation to in-house counsel at Sprint who discusses the issues with the Assistant U.S. 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.

Sprint's legal standard for each type of request was described in our submission to you last year.

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, Sprint's processes require law enforcement to fax in a form that Sprint uses 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.

Sprint's practices in responding to law enforcement requests have not changed since its May 2012 response.

6. *Did your company encounter misuse of cell phone tracking by police departments during 2012? If yes, in what ways has tracking been misused? And if yes, how has your company responded?*

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.

7. *Does your company have knowledge of law enforcement authorities that use their own tracking equipment (e.g., Stingray phone trackers)? If yes, please explain. Does your company cooperate with law enforcement that uses its own tracking equipment? If yes, how?*

Sprint is aware that such devices exist. Sprint does not provide any guidance on the usage of such devices. Any subsequent law enforcement agencies' usage of data lawfully provided by Sprint in using their own tracking devices is beyond Sprint's knowledge or control.

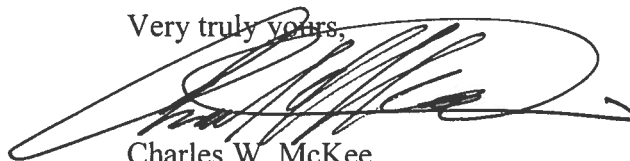
8. *In 2012, did your company receive money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money did your company receive? And if yes, how much does your company typically charge for specific services (please refer to the list in 1(a) above)?*
- a. *Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charge fees for emergency cell phone tracking requests from police departments?*
- b. *Please include any written schedule of any fees that your company charges law enforcement for these services.*

As we discussed in our submission last year, Sprint collects fees that are fully permitted by law. Attached is our current fee schedule, which is unchanged since last year. We would be happy to meet with you to discuss this issue further.

\* \* \*

I hope this letter explains Sprint's obligations to respond to law enforcement demands and answers your questions regarding our practices. The law is quite clear on the duties and obligations Sprint has in responding to law enforcement demands for customer information, with the exception of 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,



Charles W. McKee

Attachment

## Electronic Surveillance Fee Schedule

Type of Request	Fee	Notes
<ul style="list-style-type: none"> <li>- Pen Register Trap &amp; Trace (PRTT)</li> <li>- Wiretaps</li> </ul> <p><i>Note: A PRTT is a single data channel. A wiretap is a single data &amp; content channel.</i></p>	<p>1) Implementation fee per each voice or Push-to-Talk (PTT) intercept: - \$342.11</p> <p>2) Daily maintenance per each voice or PTT intercept: - \$10 (this includes 2nd set of IDs &amp; PWs)</p> <p><i>NOTE: Other technologies like femtocell, 3G, 4G, or text messaging are included in above rate unless provisioned without voice or PTT</i></p>	<ul style="list-style-type: none"> <li>- Implementation fee is a flat rate.</li> <li>- Daily maintenance covers all electronic surveillance maintenance on intercepts including upgrades, number changes, extensions, etc.</li> <li>- Exigent intercepts are free of charge until Sprint receives a court order.</li> </ul>
Late extension to intercept (LEA sends CALEA request after prior surveillance has expired)	Applicable implementation fee.	Daily maintenance applies.
Precision Location	<ul style="list-style-type: none"> <li>- Manual requests are \$20 for each time we provide location per #.</li> <li>- L-Site is unlimited requests for \$30 a month per #.</li> </ul> <p><i>NOTE: No fee in exigent, PSAP, or customer consent situations.</i></p>	Provides real-time precise location information on mobile device.
<ul style="list-style-type: none"> <li>- Electronic Communications in Storage (ECS)</li> <li>- Contemporaneous Billing</li> <li>- Cell site / sector</li> </ul>	<p>\$30 per case hour worked. Minimum of 1 hour per case plus \$7.50 for each 15 minutes worked.</p> <p><i>NOTE: No fee in Exigent, PSAP, or customer consent situation.</i></p>	<ul style="list-style-type: none"> <li>- Stored Includes text messages, voice mail retrieval, stored photo/video, historical e-mail.</li> <li>- Cell site / sector provide real-time cell site / sector of requested #.</li> </ul>
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.

Effect August 1, 2010



**Sprint Nextel**  
Suite 700  
900 7th Street, NW  
Washington, DC 20001  
Office: (703) 433-3786  
Fax: (202) 585-1940

**Charles W. McKee**  
Vice President - Government Affairs  
Federal and State Regulatory  
charles.w.mckee@sprint.com

October 25, 2013

The Honorable Edward J. Markey  
United States Senate  
218 Russell Senate Office Building  
Washington, DC 20510-2107

Dear Senator Markey:

Thank you for your September 12, 2013, letter to Dan Hesse, CEO of Sprint Corporation ("Sprint"). Sprint welcomes the opportunity to provide you additional information about the circumstances under which wireless carriers provide customer information to law enforcement. Sprint takes seriously its dual responsibilities of responding to lawful inquiries while at the same time safeguarding our customers' privacy.

In response to your letter last year, Sprint provided detailed background information about the various statutes governing Sprint's responsibilities to provide information to law enforcement. In addition, Sprint described its procedures for collecting customer information and the limits of its capabilities. Because there have been no material changes in either the law or Sprint's processes in the last year, Sprint does not repeat that background information here. However, the legal uncertainty in this area has not changed, and Sprint again urges Congress to clarify the legal requirements regarding the disclosure of location information to law enforcement personnel. Competing and at times contradictory legal standards often govern this important issue.

### **RESPONSES TO YOUR SPECIFIC QUESTIONS**

1. *In 2012, how many total requests did you company receive from law enforcement to provide information about your customers' phone usage?*
  - a. *Within that total, please list the amount of requests your company received for each type of usage, including but not limited to the following: 1) Geolocation of device (please distinguish between historical and real-time; 2) Call detail records (i.e. pen register and trap and trace); 3) Text message content; 4) Voicemail; 5) Cell tower dumps; 6) Wiretapping; 7) Subscriber information; 8) Data requests (e.g., Information on URLs visited).*
  - b. *Within that total, how many of the requests were made in emergency circumstances and how many were in non-emergency situations?*
  - c. *Within that total, how many of the requests did your company fulfill and how many did it deny? If it denied any requests, for what reasons did it issue those denials?*
  - d. *Within that total, please breakdown how many of the requests were made by Federal authorities, how many by state authorities, and how many by local authorities.*

In reviewing the publication of the wireless carriers' responses to your data requests last year, it is apparent that there are no uniform standards by which the various carriers catalog these requests, and the responses to your inquiry varied widely. For example, is a subpoena seeking information on more than one telephone number considered a single request or multiple requests? If an order is issued that extends a current wiretap, is that a second request or should it be discounted because a previous request had been issued? Because of this lack of uniformity, the numbers provided in response to this question will not be comparable across carriers.

In addition, Sprint does not track the information you have requested in the manner you describe and due to system limitations, Sprint is unable to provide even estimates for some of the information you request. Sprint does track the work-effort of the analysts who implement certain law enforcement requests for information, however, and therefore can provide that in 2012, Sprint:

- Implemented approximately 17,400 wiretaps, counting each service (data, voice, push-to-talk, text messages) as a separate wiretap implementation
- Implemented approximately 22,000 pen register/trap and trace (PR/TT) devices, counting each service (data, voice, push-to-talk) as a separate PR/TT implementation
- Provided real time or precise location information to law enforcement approximately 67,000 times
- Provided information to PSAPs/911 approximately 53,000 times
- Provided cell site information in connection with a PR/TT or a wiretap approximately 13,000 times
- Provided approximately 6000 cell tower searches to law enforcement agencies.
- Provided information to law enforcement in an emergency or "exigent" situation approximately 8500 times

Sprint does not maintain information in a readily accessible manner on the type of law enforcement agencies making these requests or on how many requests Sprint denied (and for what reasons). Providing that type of information would be unduly burdensome and require a manual review process of thousands of requests to determine the proper response.

2. *For each type of usage in 1(a), how long does your company retain the records?*

Sprint's standard retention period for law enforcement requests is 18 months.

3. *What is the average amount of time law enforcement requests for one cell tower dump (e.g., one hour, 90 minutes, two hours, etc.)? For each hour of a cell tower dump that your company provides, on average how many mobile device numbers are turned over to law enforcement?*

Sprint receives requests for "tower dumps" from federal, state, and local law enforcement agencies. Sprint does not track the average duration of each dump nor the average number of mobile device numbers that are provided to law enforcement in response to each such request.

4. *In 2012, how many requests did your company receive under Section 215 of the Patriot Act?*

Section 215 of the Patriot Act, codified at 50 U.S.C. § 501 *et seq.*, prohibits Sprint from disclosing “to any other person ... that the Federal Bureau of Investigation has sought or obtained tangible things under this section.” *Id.* § 501(d). Sprint, therefore, cannot provide any information about requests under Section 215, including whether or not Sprint has received such a request.

5. *What protocol or procedure does your company employ when receiving these requests?*

- a. *What legal standard do you require law enforcement to meet for each type of usage in 1(a)?*
- b. *Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency tracking requests? If yes, what are the distinctions?*
- c. *Have any of these practices changed since your May 2012 correspondence?*

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 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 retains 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 managers and supervisors.

This entire team 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 a Sprint analyst 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 in an escalation to in-house counsel at Sprint who discusses the issues with the Assistant U.S. 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.

Sprint's legal standard for each type of request was described in our submission to you last year.

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, Sprint's processes require law enforcement to fax in a form that Sprint uses 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.

Sprint's practices in responding to law enforcement requests have not changed since its May 2012 response.

6. *Did your company encounter misuse of cell phone tracking by police departments during 2012? If yes, in what ways has tracking been misused? And if yes, how has your company responded?*

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.

7. *Does your company have knowledge of law enforcement authorities that use their own tracking equipment (e.g., Stingray phone trackers)? If yes, please explain. Does your company cooperate with law enforcement that uses its own tracking equipment? If yes, how?*

Sprint is aware that such devices exist. Sprint does not provide any guidance on the usage of such devices. Any subsequent law enforcement agencies' usage of data lawfully provided by Sprint in using their own tracking devices is beyond Sprint's knowledge or control.

8. *In 2012, did your company receive money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money did your company receive? And if yes, how much does your company typically charge for specific services (please refer to the list in 1(a) above)?*
- a. *Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charge fees for emergency cell phone tracking requests from police departments?*
- b. *Please include any written schedule of any fees that your company charges law enforcement for these services.*

As we discussed in our submission last year, Sprint collects fees that are fully permitted by law. Attached is our current fee schedule, which is unchanged since last year. We would be happy to meet with you to discuss this issue further.

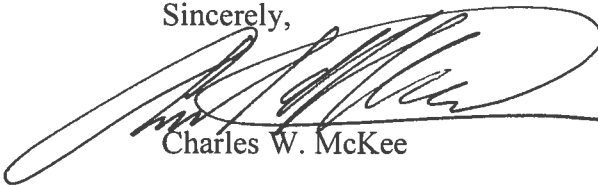
\* \* \*

I hope this letter explains Sprint's obligations to respond to law enforcement demands and answers your questions regarding our practices. The law is quite clear on the duties and obligations Sprint has in responding to law enforcement demands for customer information, with the exception of 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 Honorable Edward J. Markey  
October 25, 2013  
Page 5

the law to provide certainty for all stakeholders. If Sprint can be of further assistance to you in this regard, please let me know.

Sincerely,

A handwritten signature in black ink, appearing to read "Charles W. McKee", written over a horizontal line. The signature is fluid and cursive.

Charles W. McKee

Attachment

## Electronic Surveillance Fee Schedule

Type of Request	Fee	Notes
<ul style="list-style-type: none"> <li>- Pen Register Trap &amp; Trace (PRTT)</li> <li>- Wiretaps</li> </ul> <p><i>Note: A PRTT is a single data channel. A wiretap is a single data &amp; content channel.</i></p>	<p>1) Implementation fee per each voice or Push-to-Talk (PTT) intercept: - \$342.11</p> <p>2) Daily maintenance per each voice or PTT intercept: - \$10 (this includes 2nd set of IDs &amp; PWs)</p> <p><i>NOTE: Other technologies like femtocell, 3G, 4G, or text messaging are included in above rate unless provisioned without voice or PTT</i></p>	<ul style="list-style-type: none"> <li>- Implementation fee is a flat rate.</li> <li>- Daily maintenance covers all electronic surveillance maintenance on intercepts including upgrades, number changes, extensions, etc.</li> <li>- Exigent intercepts are free of charge until Sprint receives a court order.</li> </ul>
Late extension to intercept (LEA sends CALEA request after prior surveillance has expired)	Applicable implementation fee.	Daily maintenance applies.
Precision Location	<ul style="list-style-type: none"> <li>- Manual requests are \$20 for each time we provide location per #.</li> <li>- L-Site is unlimited requests for \$30 a month per #.</li> </ul> <p><i>NOTE: No fee in exigent, PSAP, or customer consent situations.</i></p>	Provides real-time precise location information on mobile device.
<ul style="list-style-type: none"> <li>- Electronic Communications in Storage (ECS)</li> <li>- Contemporaneous Billing</li> <li>- Cell site / sector</li> </ul>	<p>\$30 per case hour worked. Minimum of 1 hour per case plus \$7.50 for each 15 minutes worked.</p> <p><i>NOTE: No fee in Exigent, PSAP, or customer consent situation.</i></p>	<ul style="list-style-type: none"> <li>- Stored Includes text messages, voice mail retrieval, stored photo/video, historical e-mail.</li> <li>- Cell site / sector provide real-time cell site / sector of requested #.</li> </ul>
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.

Effect August 1, 2010