

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of )  
)  
Petition for Expedited Rulemaking to ) RM 11376  
Establish Technical Requirements and )  
Standards Pursuant to Section 107(b) of the )  
Communications Assistance for Law )  
Enforcement Act )

**COMMENTS OF SPRINT NEXTEL**

Sprint Nextel Corporation (“Sprint Nextel”), pursuant to the Federal Communication Commission’s (“FCC” or “Commission”) *Public Notice* DA 07-2522 dated June 21, 2007, hereby respectfully submits its comments on the Petition for Expedited Rulemaking to Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act, (“Petition”), filed by the Department of Justice (“DOJ”) on May 15, 2007.

**I. INTRODUCTION**

According to the DOJ, “American National Standard Institute (“ANSI”) J-STD-025-B, the CALEA [Communications Assistance for Law Enforcement Act] standard for CDMA2000 packet data wireless services (“J-STD-025-B”),” Petition at 1-2, is deficient “because it fails to include certain assistance capability requirements mandated by CALEA Section 103.” Petition at 4. Specifically, the DOJ claims that the J-STD-025-B “does not include...(1) packet activity reporting; (2) timing information (time stamping); (3) all reasonably available mobile handset location information at the beginning and the end of a communication; and (4) adequate security, performance and reliability requirements.” Petition at 4-5 (footnote omitted). The DOJ goes on to argue that

“[w]ithout these required capabilities, law enforcement will be unable to carry out LAES [lawfully authorized electronic surveillance] fully and effectively.” Petition at 5. Thus, the DOJ requests that the Commission exercise its authority under CALEA Section 107(b) to conduct a rulemaking with the goal of issuing rules mandating that these capabilities be made part of the J-STD-025-B CDMA2000 packet data wireless services.

Under Section 107(b) of CALEA, a government agency, *inter alia*, that believes that a standard developed by industry associations or standard-setting organization is deficient must petition the Commission “to establish, by rule, technical requirements or standards” that would cure such deficiency. For its part, the Commission must ensure that any revisions to the industry standard being requested by the government agency “(1) meet the assistance capability requirements of Section 103 by cost-effective methods; (2) protect the privacy and security of communications not authorized to be intercepted; (3) minimize the cost of such compliance on residential ratepayers; (4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and (5) provide a reasonable time and conditions for compliance with and the transition to any new standard...” 47 U.S.C. §1006(b).

Sprint Nextel believes that the Commission cannot meet these statutory criteria with respect to at least two of the capabilities that the DOJ asks be made a part of the J-STD-025-B. As more fully set forth below, DOJ’s request that the J-STD-025-B be amended to include the provision of “more accurate” (Petition at 38) location information and provide for the buffering of data fall well outside carriers’ CALEA obligations.

Thus, if the Commission decides to initiate the rulemaking requested by DOJ, it cannot include these particular requests within the scope of rulemaking.<sup>1</sup>

## II. DISCUSSION

### A. Latitude And Longitude Information Of Anything Other Than The Cell Site Falls Well Outside CALEA Requirements.

There can be no dispute that the CALEA does not require the delivery of the precise location of the wireless device being used by the target of an intercept order. Previously, the Commission concluded that “location of a cell site ...at the beginning and termination of a call will give LEAs [Law Enforcement Agencies] adequate information.” *Communications Assistance for Law Enforcement Act*, 14 FCC Rcd 16794, 16816 ¶46 (1999) (*Third Report*). More importantly, the Commission went on to find that although

---

<sup>1</sup> Sprint Nextel recognizes that given its responsibilities under Section 107(b) of CALEA, the Commission may have to institute a rulemaking to examine whether to require modifications to the J-STD-025-B to accommodate the other requests by DOJ that may arguably be within the scope of CALEA. Sprint Nextel assumes that if the Commission determines after a thorough review of the requests in such rulemaking that the J-STD-025-B should be modified in certain respects, the Commission will direct the appropriate standards-setting bodies to begin the process to revise the J-STD-025-B appropriately that could be adapted to all packet technologies and will not, as DOJ seems to suggest, prescribe rules limited only to packet data transmitted via one particular technology – CDMA2000. Indeed, given their expertise and the fact that there is broad participation by industry members, standards-setting bodies are the appropriate fora for addressing the highly technical and evolving requirements necessary to support law enforcement’s electronic surveillance needs. Moreover, if the Commission does require modifications to the J-STD-025-B, it must give the carriers adequate time to meet the revised standard. Sprint Nextel suggests carriers be given at least 24 months to comply with a revised J-STD-025-B. The multiple network modifications and testing necessary to comply with some of the DOJ’s requests simply cannot be implemented within the 12-month period that the DOJ has proposed.

“a capability that identifies location more precisely would be useful to LEAs...such a capability pose[d] difficulties that could undermine individual privacy.” *Id.*

Despite this finding and the Commission’s apparent concern for citizens’ privacy rights, the DOJ nonetheless insists that LEAs “are entitled, pursuant to lawful authorization” (Petition at 27), to receive the precise location of the handset of the target both at the beginning and termination of the call.<sup>2</sup> This is so, according to the DOJ, because such information is “reasonably available” call-identifying information (“CII”) which carriers are required to provide to law enforcement under CALEA. *See* 47 U.S.C. §1002.<sup>3</sup> Petition at 28.

The DOJ’s argument appears to be based on the view that because of advances in “[l]ocation identification technology ... the types of signaling information reasonably available to carriers regarding handset location have changed dramatically” and carriers now have the “ability to precisely locate a wireless subscriber.” Petition at 32. The DOJ attributes these advances to “the Commission’s E-911 Phase II wireless services mandate,

---

<sup>2</sup> The Commission stated that its decision that CALEA does not require that carriers provide precise location information of the target’s handset “does not preclude LEAs from requesting legal authority to acquire more specific location information in particular circumstances.” *Third Report*, 14 FCC Rcd at 16816 ¶46. Although the DOJ quotes this statement, it does not explain how this statement supports its view that carriers are required by CALEA to deliver the precise location of the target’s handset to law enforcement. Nor could it since this statement is nothing more than the Commission’s recognition that a carrier should comply with a court order to the best of its ability. It has nothing to do whether the delivery of precise handset location information is required by CALEA.

<sup>3</sup> CII is “dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.” 47 U.S.C. §1001(2).

which requires wireless carriers to be capable of providing the precise latitude, longitude and altitude location information for wireless subscribers' handsets." Petition at 32-33.

The DOJ then claims that carriers now "routinely use their E-911 Phase II location information capability to assist them in other business and commercial operations such as call completion and network management" and to offer "new and improved wireless location service[s] ...to their subscribers." Petition at 33.

The DOJ's assumptions about the carrier use of E911 location information are misplaced. The fact that carriers have installed a "location information capability" into their handsets to comply with Commission's E-911 Phase II mandate to deliver information giving the latitude and longitude information of the caller's handset to the public safety answering point ("PSAP") – Sprint Nextel has installed global positioning satellite ("GPS") chips into its handsets to provide this capability – does not necessarily mean that carriers now routinely receive this information from handsets on all calls or use the information for call processing and routing. In Sprint Nextel's case, it does not use GPS technology in that manner. Indeed, only the dialing of 911 will cause the handset to generate a "GPS fix," and this fix is nothing more than data delivered to the PSAP.<sup>4</sup> Signaling information to enable carriers to process and route calls, even 911 calls,

---

<sup>4</sup> It is true that Sprint Nextel uses GPS to offer Location Based Services (LBS), but latitude and longitude information is embedded in the packets used in an LBS application and is not signaling information used by the carrier to identify "the origin, direction, destination, or termination" of the LBS-capable handset. In other words, the location information that an LBS provides is not CII.

continue to be based only on the cell site and cell sector coordinates; not the GPS coordinates of the handset.<sup>5</sup>

Thus, contrary to the DOJ's belief, there has not been any change in the signaling information, dramatic or otherwise, used to process or route a wireless call, even with the addition of GPS technology to certain handsets. There is no additional CALEA-mandated information available to DOJ as a result of GPS-enabled handsets.

**B. The DOJ's Attempt To Shift The Costs Of the Facilities Used In A CALEA Intercept To Carriers Must Be Rejected.**

The DOJ asks the Commission to require the delivery of packets "to a law enforcement co-located collection device or carrier-provided buffering and retrieval of LAES over a secure VPN [virtual private network]." Petition at 49 n. 110. If adopted, law enforcement would no longer have to obtain the dedicated facilities necessary to permit the delivery of the packets. Rather, DOJ would be able to place equipment at a carrier's data center or perhaps Mobile Switching Office ("MSO") to collect the packets for delivery to law enforcement at a later time or make carriers responsible for

---

<sup>5</sup> The DOJ argues that carriers "use the longitude and latitude location information for purposes of the identifying the 'origin' (i.e., geographic location) of the subscriber's handset ... for network management and efficiency purposes." Petition at 33 n. 80. By way of example, it states that "carriers often use the more precise information to route calls through an alternative cell tower – rather than the 'default' tower or one to which the call would ordinarily have been routed based on its proximity to the caller – in order to reduce the burden on a particular tower for network efficiency." *Id.* The DOJ does not provide the Commission with any evidence that would support this statement, which, in Sprint Nextel's case, is incorrect. Sprint Nextel does not use GPS information for call routing or re-routing. Traffic management is purely a function of the analysis of the load placed on particular sectors of particular cell sites and the GPS fix of a particular handset even assuming it is generated for every call – and it is not – is not needed for such analysis.

temporarily storing and then forwarding, *i.e.*, buffering, the packets to data to law enforcement over a secure VPN.

The difficulty with the DOJ's request is that it is contrary to the plain language of the CALEA statute. Specifically, under CALEA Section 103(a)(3), 47 U.S.C. §1002(a), law enforcement is required to obtain "the equipment, facilities or services" necessary to permit the "deliver[y] [of] intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization... to a location other than the premises of the carrier." Thus, to grant the DOJ's request, the Commission would have to ignore this statutory provision.

Even setting aside the legal problems with the request, the DOJ also has not provided any policy justification. The DOJ claims that its request for "near-real-time delivery of communications content to a law enforcement co-located collection device, or carrier provided buffering would be "cost-effective," and would "solve" what the DOJ says is a data reliability problem. Petition at 49 and n. 110. This justification, such as it is, is without merit. While it is true that shifting law enforcement's costs to carriers and their customers is a "cost-effective" solution at least for law enforcement, the proposal would not result in an overall efficiency gain. Moreover, shifting of law enforcement's costs to carriers is barred by statute.

As for the so-called data reliability problem, Sprint Nextel would note that today delivery of all data to an LEA is done in secure manner requested by the LEA. As a general matter, Sprint Nextel sends wiretap information either over dedicated connections or over IPSec with encryption links.

Sprint Nextel agrees that the reliability of data transmission to law enforcement is critical. To that end and unless otherwise requested, Sprint Nextel typically delivers data streams to law enforcement using Transmission Control Protocol (“TCP”). By definition, TCP ensures reliable service by retransmitting data when an initial transmission results in an error. Thus, LEAs are already assured they receive 100% reliable communications by using TCP as the transport protocol.

That said, TCP requires that the transmission and receiving devices operate at nearly the same data rate; otherwise, data can be lost during the transmission. When routers placed at either end of a transmission reach their capacity, the routers themselves will begin to drop packets of data. Again, however, CALEA clearly places the responsibility on law enforcement to procure the bandwidth necessary to ensure capture of all wiretap information generated by a single or multiple targets of a data wiretap. Nowhere does the statute permit the shifting of these costs from law enforcement to the carriers and their customers.

In any event, the two alternatives suggested by the DOJ to avoid its costs are simply not practical. Collocating equipment would require that carriers permit access to LEAs to space over which they themselves may not control.<sup>6</sup> Carriers often lease space in areas in which they are a tenant, not the owner. Law enforcement would have to negotiate separate rights with the property owners in order to access these facilities.

---

<sup>6</sup> The collocation alternative, of course, assumes that space exists (as well as the necessary power) to permit the installation of additional equipment. In many cases, space within data centers and MSOs is at a premium, and there simply may not be physical space available for installation of any third party equipment.

Moreover, Sprint Nextel treats security at its data centers and MSOs very seriously. Allowing access to what will likely be law enforcement agencies' contractors – rather than law enforcement agents themselves – could compromise the security systems Sprint Nextel has put in place to ensure the privacy and reliability of its customers' communications.

The DOJ's "buffering" alternative is equally flawed. Although the buffering of the data would enable law enforcement to use less bandwidth to accommodate the packets being transmitted, it exposes carriers to potential liability for failures in the buffering equipment used and the loss of intercepted evidence that could result. And, it may require that carrier employees spend more time in court testifying as to the carrier's processes for ensuring that the buffered data are authentic. Since under Title 18 carriers have the right to collect these additional costs from law enforcement, any savings that law enforcement may realize through the DOJ's attempt to shift costs to carriers and their customers may well be illusory.

### III. CONCLUSION

For the reasons stated above, if the Commission decides to issue a notice of proposed rulemaking in response to DOJ's petition, it cannot include within the scope of such rulemaking the DOJ's requests that (1) latitude and longitude information of the target's handset be provided as part of a CALEA-based interception; and (2) that carriers, rather than the government, pick up the costs for ensuring that that packets are not dropped or lost during the course of a wiretap.

Respectfully submitted,

SPRINT NEXTEL CORPORATION



Laura Carter

Anna M. Gomez

Michael B. Fingerhut

2001 Edmund Halley Drive

Reston, Virginia 20191

(703) 592-5112

Its Attorneys

**CERTIFICATE OF SERVICE**

I, Jo-Ann Monroe, do hereby certify that, on this 25th day of July 2007, copies of the foregoing "Comments of Sprint Nextel," were served electronically, or by U.S. first-class mail, postage prepaid, to the following:

Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D.C. 20554  
(Via ECFS)

Derek Poarch, Chief  
Public Safety and Homeland Security  
Bureau  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D.C. 20554  
[Derek.Poarch@fcc.gov](mailto:Derek.Poarch@fcc.gov)

Dana Shaffer, Deputy Bureau Chief  
Public Safety and Homeland Security  
Bureau  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D.C. 20554  
[Dana.Shaffer@fcc.gov](mailto:Dana.Shaffer@fcc.gov)

Tom Beers, Deputy Chief  
Policy Division  
Public Safety and Homeland Security  
Bureau  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D.C. 20554  
[Tom.Beers@fcc.gov](mailto:Tom.Beers@fcc.gov)

David O. Ward, Senior Attorney  
Public Safety and Homeland Security  
Bureau  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D.C. 20554  
[David.Ward@fcc.gov](mailto:David.Ward@fcc.gov)

Sigal P. Mandelker  
Deputy Assistant Attorney General  
Criminal Division  
United States Department of Justice  
950 Pennsylvania Avenue, N.W.  
Washington, D.C. 20530

Elaine N. Lammert  
Deputy General Counsel  
Office of the General Counsel  
Federal Bureau of Investigation  
United States Department of Justice  
935 Pennsylvania Avenue, N.W.  
Washington, D.C. 20535

Charles M. Steele  
Chief of Staff  
National Security Division  
United States Department of Justice  
950 Pennsylvania Avenue, N.W.  
Washington, D.C. 20530

Michael L. Ciminelli  
Deputy Chief Counsel  
Office of Chief Counsel  
Drug Enforcement Administration  
United States Department of Justice  
Washington, D.C. 20537

Best Copy and Printing, Inc.  
Portals II  
445 12th Street, S.W., Room CY-B402  
Washington, D.C. 20554  
[fcc@bcpiweb.com](mailto:fcc@bcpiweb.com)

  
Jo-Ann Monroe