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

In the Matter of	)	
	)	
Petition for Rulemaking on Compliance by Carriers with Relevant Statutory Provisions on Disclosure of Customer Information in 911 Emergencies	)	RM No. 10715

SPRINT COMMENTS

Sprint Corporation, on behalf of its local, long distance and wireless divisions ("Sprint"), submits these comments in response to the petition for rulemaking filed on May 2, 2003 by the National Emergency Number Association, the Association of Public-Safety Communications Officials-International, and the National Association of State Nine One One Administrators (collectively, "Public Safety Petitioners").[1] The Petitioners ask the Commission to either "open a rulemaking or issue a declaratory order as to compliance with the relevant statutory provisions on disclosure of [customer] information in 9-1-1 emergencies."[2]

I. INTRODUCTION AND SUMMARY

Sprint strives to accommodate the needs of Public Safety. In this regard, Sprint has been a leader in deploying E911 wireless capabilities. Sprint installed the nation's first operational Phase II system (Rhode Island), and has deployed Phase I systems with over 1,700 PSAPs and

[1] *See Public Notice,* Comment Sought on Petition for Rulemaking on Compliance by Carriers with Relevant Statutory Provisions on Disclosure of Customer Information in 911 Emergencies, RM-10715, DA 03-1952 (June 16, 2003).

[2] Public Safety Petition at 9.

Phase II systems with over 370 PSAPs.[3] Sprint was the first and only carrier to begin selling Phase II handsets by the Commission's deadline, and it has already sold nearly 12 million of such handsets.[4] In the context of the pending petition, Sprint was happy to provide Public Safety with its written policies on disclosure of customer specific information to 911 authorities and made itself available for further questions.[5]

Sprint agrees with the Public Safety Petitioners that clarification of the line separating customer's reasonable privacy interests and the legitimate needs of public safety would be welcome. Carriers may be able to respond more quickly and decisively to public safety inquiries if they had available to them a set of uniform and clear rules identifying what sensitive customer information may, and may not, be shared under different circumstances. Sprint has established what it believes are appropriate procedures under current law and is willing to work with Public Safety to further improve those procedures. Sprint, however, is still bound by the letter of law.

The difficulty presented by the Petition is that it is unclear that the Commission could grant it as a matter of law. Among other things, the Public Safety Petitioners ask the Commission to broaden a statutory exception contained in Section 222(d) of the Communications Act. While the Commission certainly has the authority to interpret its organic statute and while the Petitioners may very be correct that it is "unfortunate" that Congress "limit[ed] Section 222(d) disclosure to cases when the caller and the endangered person are one and the same,"[6] the fact remains that the Commission does not have the legal authority to redraw the lines that Congress has enacted.

---

[3] *See* Sprint Corporation Seventh Quarterly E911 Implementation Report, CC Docket No. 94-102, at 3 (Aug. 1, 2003).

[4] *See id.* at 2.

[5] *See* Public Safety Petition at 4 and Attachment 1.

The Public Safety Petitioners also ask the Commission to "align the criminal statues with the civil law reflected in the Communications Act," taking the view that the exceptions Congress established in the criminal code are not broad enough for public safety's purposes.[7] The Commission, however, has no authority to declare conduct legal that Congress has unambiguously determined is illegal.

As noted, the objective sought by the Public Safety Petitioners is laudable, and Sprint supports it. Sprint therefore encourages the Commission to invite the Department of Justice to submit in the public record a legal memorandum discussing carrier obligations under the nation's criminal laws to share customer information with public safety agencies and the interplay of those criminal laws with Section 222 of the Communications Act. Once this memorandum is submitted, the Commission may wish to host a workshop of public safety agencies, carriers and customer representatives to explore the alternatives that are available, both legally and operationally, so public safety's legitimate interests can be satisfied as fully as possible consistent with the criminal code and the Communications Act.

II. CARRIERS FACE A DIFFICULT TASK IN ATTEMPTING TO MEET THE NEEDS OF PUBLIC SAFETY WHILE MEETING THEIR LEGAL OBLIGATION TO PROTECT THE CONFIDENTIALITY OF THEIR CUSTOMERS' INFORMATION

As noted above, Sprint attempts to accommodate the needs of public safety. But Sprint also has a legal obligation to follow the law as set forth in the criminal code and the Communications Act (both of which are summarized below). The criminal statutes in particular are very specific as to what kind of sensitive customer information a carrier can disclose to public safety

---

[6] Public Safety Petition at 6.

[7] Public Safety Petition at 6 n.11.

personnel and in what circumstances. Carriers thus adopt reasonable safeguards to ensure they comply with all laws.

The Public Safety Petitioners' illustrative example (summarized in Exhibit A) highlights the difficult task that carriers often face. In this example, a public safety official requested information about a wireless customer who did not originate the 911 call and who was not the person at risk. As discussed more fully below, criminal statutes permit carriers to disclose customer records to public safety personnel "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."[8] In this example, the wireless carrier furnished the information requested, but it asked the public safety agency to follow up by submitting within 48 hours a subpoena or court order.[9] At a minimum, Carriers such as Sprint require that the Public Safety Agency requesting information execute a document certifying that an exigent circumstance exists. This is a common industry practice that carriers employ to help ensure there truly is an emergency "justif[ying] disclosure of the information."

The Public Safety Petitioners appear to object to the carrier requirement of a subpoena, court order or other document.[10] But without such documentation, a carrier has no means of ensuring that sensitive customer information is being sought for a life-and-death emergency and that the carrier is complying with the law.

Although obtaining a court order or subpoena is not an onerous burden, there may be other methods by which public safety agencies could obtain the information they need and at the

---

[8] 18 U.S.C. § 2702(c)(4).

[9] Public safety and other government agencies can require a carrier to disclose customer records with a warrant, a court order or administrative subpoena. *See* 18 U.S.C. § 2703(c),

same time allow carriers to comply with their obligations under Section 222 of the Act and Title 18 of the United States code. It also may be that public safety needs could be addressed simply by the adoption of a standard subpoena form that would be available to all public safety agencies. Sprint encourages the Commission to investigate whether there are any such alternative methods and if such methods are found to exist, take the appropriate steps to ensure that such methods can be utilized

III. THE COMMISSION DOES NOT POSSESS THE LEGAL AUTHORITY TO REVISE CRIMINAL STATUTES

The Electronic Communications Privacy Act ("ECPA") generally prohibits telecommunications carriers from divulging any customer information to any governmental entity. Specifically, 18 U.S.C. § 2702(a)(3) provides:

> Except as provided in subsection (b) . . . a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental agency.

This criminal statute, the Department of Justice ("DoJ") has observed, "creates statutory privacy rights for customers and subscribers."[11] A carrier contravening the provisions of the ECPA may be fined, imprisoned and/or subjected to civil liability (including payment of attorneys' fees).[12]

Congress has established several exceptions to this prohibition where a carrier "may divulge" its customers records to a governmental entity upon request. Under one of the excep-

---

[10] *See* Public Safety Petition at Exhibit A ("Now I have Carrier X hounding me for a court order or subpoena.").

[11] Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, at § III.A (July 2002)("DoJ ECPA Manual"), *available at* www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm.

[12] *See* 18 U.S.C. §§ 2701, 2707.

tions, a carrier "may divulge a record or other information pertaining to a subscriber to or customer of such service . . . to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."[13]

Two points bear emphasis concerning this particular exemption. First, the circumstances where disclosure is permitted is limited in scope – namely, the carrier must "reasonably believe" that there exists an emergency involving "immediate danger of death or serious physical injury" and that this danger "justifies disclosure." Second, even if these circumstances are present, it is the carrier's decision alone to decide whether or not to disclose the requested customer information.[14] If a governmental entity wants to require a carrier to disclose its customer's records, the requesting agency must comply with the procedures set forth in a related statutory provision.[15] For example, a government agency wanting to obtain a customer's name and address must first secure a subpoena for such information.[16]

The Public Safety Petitioners state that the "immediate danger of death or serious physical injury" limitation contained in the ECPA "seems unwarranted" and should be broadened to include "endangered property":

> [R]eports of fire or apparent burglary often present no threat to life but they surely describe property at risk. To the 9-1-1 call taker, saving property remains highly important even if lower in priority than saving lives. It makes little sense to dif-

---

[13] 18 U.S.C. § 2702(c)(4). This provision was added by the USA PATRIOT Act of 2001. *See* Pub. L. 107-56, § 212(a)(1)(E).

[14] Importantly, Section 2702 of the criminal code is titled, "Voluntary Disclosure of Customer Communications or Records."

[15] *See* 18 U.S.C. § 2703, titled, "Required Disclosure of Customer Communications or Records."

[16] *See* 18 U.S.C. § 2703(c)(2).

> ferentiate the disclosure of customer information based on whether property or lives may be at risk.[17]

The Public Safety Petitioners therefore ask the Commission to direct carriers to change their release forms so as to permit the release of sensitive customer information in circumstances where there is no "immediate danger of death or serious physical injury."[18]

The Commission, of course, does not generally interpret our nation's criminal laws,[19] and the DoJ has observed that the ECPA is "an unusually complicated statute."[20] More importantly, however, the Commission does not possess the statutory authority to rewrite the nation's criminal laws.[21] Yet, to grant the Public Safety Petitioners' request, the Commission would necessarily be required to re-write the criminal code to authorize release of sensitive customer information when there is no "immediate danger of death or serious physical injury." Sprint submits that the Commission lacks the requisite authority to permit conduct that is not authorized by a criminal statute.

The Public Safety Petitioners' also ask the Commission to examine the interplay of the requirements of the criminal code with the requirements of the Communications Act and to "rec-

---

[17] Public Safety Petition at 5-6.

[18] *See id.* at 7.

[19] For example, when the FCC required wireless carriers to provide PSAPs with customer location information, it did not determine that this directive was consistent with the criminal laws but rather sought a legal opinion from the DoJ. *See First E911 Order*, 11 FCC Rcd 18676, 18727 ¶ 98 (1996). *See also* DoJ, Memorandum Opinion for John D. Keeney, Acting Assistant Attorney General (Sept. 10, 1996), submitted in the record of CC Docket No. 94-102 on December 13, 1996; *Public Notice,* Memorandum Opinion Issued by Department of Justice Concludes That Commission's Recently Adopted Wireless Enhanced 911 Rules Are Consistent with Wiretap Act, 11 FCC Rcd 17305 (1996); *First E911 Reconsideration Order,* 12 FCC Rcd 22665, 22728-29 ¶ 131, 22734 ¶ 142 (1997).

[20] DoJ ECPA Manual at § III.A.

[21] *See, e.g., USTA* v. *FCC,* 227 F.3d 450, 465 (D.C. Cir. 2000)("CALEA authorizes neither the Commission nor the telecommunications industry to modify either the evidentiary standards or procedural safeguards for securing legal authorization to obtain packets from which call content has not been stripped, nor may the Commission require carriers to provide the government with information that is 'not authorized to be intercepted.'").

oncile" any differences between the two sets of statutes.[22] Again, the Commission does not possess the requisite expertise to interpret definitively the requirements of the criminal code. Accordingly, as Sprint recommends in Part V, the Commission should refer these issues to the Department of Justice.

IV. THE COMMISSION LACKS THE STATUTORY AUTHORITY TO EXPAND THE LIMITATIONS IMPOSED IN THE COMMUNICATIONS ACT

Section 222 of the Communications Act imposes on carriers the duty to protect the confidentiality of customer proprietary network information ("CPNI"),[23] a category that encompasses customer location information.[24] Congress has established several exceptions to this confidentiality duty. Among other things, a carrier may release "call location information concerning the user of a commercial mobile service" to public safety personnel "in order to respond to the user's call for emergency services."[25] In other words, as the Public Safety Petitioners' acknowledge, this exception applies only when "the caller and the endangered person are one and the same."[26]

The Public Safety Petitioners state that this "user" limitation is "unfortunate":

> Often, victims are unable to dial for help. Instead, aid is summoned by persons acting on their behalf or by "Good Samaritans."[27]

---

[22] Public Safety Petition at 9.

[23] *See* 47 U.S.C. § 222(a)("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, . . . customers . . . .").

[24] *See* 47 U.S.C. § 222(h)(1)("The term 'customer proprietary network information' means (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.").

[25] 47 U.S.C. 222(d)(4)(A). A carrier may also release call location information "to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm." *See id.* at § 222(d)(4)(B).

[26] Public Safety Petition at 6.

[27] Public Safety Petition at 6.

The Public Safety Petitioners therefore ask the Commission to determine whether "the term 'user' in Section 222(d)(4) limit[s] the disclosure of location information in 9-1-1 emergencies."[28]

The Commission certainly has the authority to interpret its authorizing statute, the Communications Act. Sprint cautions, however, that the Commission does not have unfettered discretion to construe the Act in any way it wishes.[29] As the Supreme Court has held, "if the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress."[30] The Congressional language in Section 222(d)(4)(A) contains little ambiguity regarding the kind of information carriers can provide to public safety personnel and when carriers can furnish this information. Congress has determined that carriers may disclose "call location information concerning the user of a commercial mobile service" in order "to respond to the *user's* call for emergency services."[31]

It appears that the Public Safety Petitioners believe that, in Section 222(d)(4)(A), Congress did not properly draw the line between customer privacy interests and the interests of public safety agencies. However, greater privacy interests are involved when public safety personnel are inquiring about location information concerning a person that did not originate the 911

---

[28] *Id.* at 8.

[29] *See, e.g., Maislin Industries* v. *Primary Steel,* 497 U.S. 116, 134-35 (1990)(Agency "does not have the power to adopt a policy that directly conflicts with its governing statute.").

[30] *Chevron USA* v. *Natural Resources Defense Council,* 467 U.S. 837, 842-43 (1984). *See also Amatel* v. *Reno,* 156 F.3d 192, 207 (D.C. Cir. 1998)("[A]gencies surely do not have inherent authority to second-guess Congress' calculations.").

[31] 47 U.S.C. § 222(d)(4)(A)(emphasis added).

call.[32] The important point for purposes of this petition is that "agencies surely do not have inherent authority to second guess Congress' calculations."[33]

V. A PROPOSAL TO EXPLORE PUBLIC SAFETY'S CONCERNS

While Sprint does not believe that the Commission can grant the Public Safety Petition in its current form, it does agree that Public Safety has raised issues that merit further exploration. The first and most important step is to understand the requirements of the criminal code and the interplay of that code with the Communications Act. Sprint urges the Commission to follow the same procedure it utilized following adoption of its original wireless E911 rules: ask the Department of Justice to prepare a legal opinion that would be submitted in the public record.[34]

It is only when legal requirements and limitations are known that public safety agencies and carriers can meaningfully begin discussing possible changes in current practices to better meet public safety needs, while still protecting the legitimate privacy interests of customers as set forth in the Section 222 of the Act and in Title 18 of the U.S. Code. Sprint therefore recommends that, once the Justice Department completes its legal memorandum, the Commission host an open workshop of public safety officials, carriers and consumer representatives so any public safety concerns can be addressed. This workshop may be more focused (and, hence, more productive) if the Commission first seeks public comment on the DoJ legal opinion, as the comments submitted could help identify the issues that the workshop should explore.

It may be that the needs of public safety can be accommodated under existing law. If not, attendees at the workshop can attempt to craft proposed language that would amend existing

---

[32] As the DoJ determined in its 1996 opinion, customers who initiate a 911 call have no reasonable expectation of privacy. This "implied consent" rationale does not apply when the 911 call is originated by a person other than the customer.

[33] *Amatel* v. *Reno,* 156 F.3d 192, 207 (D.C. Cir. 1998).

statutes. Sprint is confident that Congress would act promptly if presented with a consensus proposal endorsed by all involved parties.

VI. CONCLUSION

For the foregoing reasons, Sprint Corporation respectfully suggests that the Commission must deny the Public Safety Petition as presented but further recommends that the Commission adopt the proposal set forth in Part V above as a reasonable means to explore the concerns that Public Safety has raised in their Petition.

Respectfully submitted,

SPRINT CORPORATION

Luisa L. Lancetti
Vice President, PCS Regulatory Affairs
Sprint Corporation
401 9th Street, N.W., Suite 400
Washington, D.C. 20004
202-585-1923

Charles W. McKee
General Attorney
Sprint Corporation
6450 Sprint Parkway
Mail Stop: KOSPHN0212-2A553
Overland Park, KS 66251
913-315-9098

August 15, 2003

[34] *See* note 19 *supra.*

Certificate of Service

I, JoAnn Monroe, certify that on August 15, 2003, I caused a copy of the foregoing Sprint Comments to be mailed, *via* first class mail, postage prepaid, to the attorneys for the Public Safety Petitioners:

James R. Hobson
Miller & Van Easton, P.L.L.C.
1155 Connecticut Avenue, N.W., Suite 1000
Washington, D.C. 20036

Robert M. Gurss
Shook Hardy & Bacon, L.L.P.
600 14th Street, N.W., Suite 800
Washington, D.C. 2005

JoAnn Monroe