

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

In the Matter of)
)
Release of Customer Information) **RM-10715**
During 9-1-1 Emergencies)

REPLY COMMENTS OF AT&T WIRELESS SERVICES, INC.

AT&T Wireless Services, Inc. (“AWS”) hereby submits its reply comments in response to the Commission’s *Public Notice* in the above-captioned proceeding.^{1/}

INTRODUCTION AND SUMMARY

The National Emergency Number Association (“NENA”), the Association of Public Safety Communications Officials-International, Inc. (“APCO”), and the National Association of State Nine One One Administrators (“NASNA”) (collectively “Petitioners”) ask the Commission to rule that carriers can and must release location information to public safety entities even if the customer proprietary network information (“CPNI”) requested is associated with a customer who was not the caller to 911, and even if the emergency involves only a danger to property rather than a threat to life or serious injury.^{2/} Neither the plain language nor the legislative history of the relevant statutes supports Petitioners’ requested ruling. Rather, as the record demonstrates, it appears that Congress made a deliberate choice to balance the privacy interests and public safety needs of consumers by limiting the disclosure of confidential information to extremely dire emergencies or to situations in which the caller has evidenced a desire to be located by dialing

^{1/} See “Comment Sought on Petition for Rulemaking on Compliance by Carriers With Relevant Statutory Provisions on Disclosure of Customer Information in 911 Emergencies,” DA 03-1952, *Public Notice*, 18 FCC Rcd 11778 (2003).

^{2/} *Release of Customer Information During 9-1-1 Emergencies*, RM-10715, *Petition for Rulemaking* at 5-7 (filed May 2, 2003) (“*Petition*”).

911.^{3/} As CTIA and Sprint explain, to the extent Petitioners believe Congress has given privacy concerns too much weight, they should pursue any necessary statutory changes directly with the lawmakers.

Nor is there any basis for granting the Electronic Privacy Information Center's ("EPIC's") proposal to afford greater privacy protection to customers that make calls to 911 on behalf of others. Not only is EPIC's requested change unwarranted from a policy perspective, it would be impossible to implement technologically. Given the way Phase I and Phase II E911 systems work, there is simply no opportunity for either carriers or PSAPs to inquire of the caller whether he is experiencing the emergency himself and whether he would like to withhold delivery of his location information. Attempting to insert such a step into the automatic call/data transmission process would completely undermine the effectiveness of the E911 system and thereby endanger the lives it is intended to protect.

I. THE STATUTORY FRAMEWORK IS CLEAR AND SHOULD NOT BE ALTERED BY THE COMMISSION

The general rule under the statutes referenced by Petitioners is that, absent customer consent or a court order, a wireless carrier may not provide customer location information to PSAPs or other government entities.^{4/} Compliance with this requirement is particularly important because, as Sprint notes, without a "subpoena, court order or other document . . . a

^{3/} CTIA at 3; Sprint at 10.

^{4/} See Memorandum Opinion for John C. Keeney Acting Assistant Attorney General, Criminal Division from Richard L. Shiffrin, Deputy Assistant Attorney General, U.S. Dept. of Justice, Office of Legal Counsel, Sept. 10, 1996 ("DOJ Memo"). See also "Memorandum Opinion Issued by the Department of Justice Concludes that the Commission's Recently Adopted Wireless Enhanced 911 Rules are Consistent with Wiretap Act," DA 96-2067, *Public Notice* (rel. Dec. 10, 1996); see also CTIA at 6 ("Disclosure of . . . information . . . requires the government to obtain a court order for disclosure based on specific and articulable facts that the information is relevant and material to an ongoing criminal investigation."); Sprint at 4 n.9, 6 ("Public safety and other government agencies can require a carrier to disclose customer records with a warrant, a court order, or administrative subpoena.").

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.”^{5/} In addition, telecommunications providers that fail to comply with these requirements may face criminal and civil penalties.^{6/} Carriers, therefore, “have a strong incentive to protect against unlawful disclosure of customer records and to rely on legal process in responding to any governmental request for such information.”^{7/}

Notwithstanding its general policy in favor of safeguarding privacy, Congress has recognized that disclosures made without prior explicit consent or court order are warranted in certain circumstances. Therefore, the Communications Act permits disclosure of a caller’s location information to a PSAP if he dials 911 and the Electronic Communications Privacy Act (“ECPA”) permits carriers to provide CPNI to a PSAP if the carrier reasonably believes there is an immediate threat to life that requires disclosure without delay. Congress, however, has carefully circumscribed the situations in which the urgent need for disclosure of consumer information is deemed to overcome a customer’s ability to control the release of such information.

Specifically, under section 222(d)(4) of the Communications Act, a wireless carrier may disclose location information to PSAPs “in order to respond to the user’s call for emergency services.”^{8/} In enacting this provision, Congress made clear that the delivery of this information

^{5/} Sprint at 4.

^{6/} 18 U.S.C. §§ 2701, 2703(e), 2707; Sprint at 5; CTIA at 6.

^{7/} CTIA at 7.

^{8/} See 47 U.S.C. § 222(d)(4) (emphasis added). The term “emergency services” is defined as “9-1-1 emergency services and emergency notification services.” 47 U.S.C. § 222(h)(5). See also Sprint at 8 (“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 . . . [and] this exception applies only when the caller and the endangered person are one and the same”) (internal quotations omitted).

is restricted to the “location of a cellular or other personal wireless user.”^{9/} As CTIA points out, section 222(d)(4) essentially codifies a prior finding by the Department of Justice (“DOJ”) that a warrant or court order is not necessary under 18 U.S.C. § 2703(c) for the Commission to require wireless carriers to pass location information to PSAPs because “by dialing 911, the caller impliedly consents to the disclosure of a caller’s physical location at the time of a 911 call.”^{10/} The DOJ concluded that a caller who dials 911 has neither an actual nor a reasonable expectation of privacy with regard to his whereabouts at the time of the call.^{11/}

Further, although section 222(d)(4) and the DOJ’s interpretive ruling would not permit a carrier to disclose location information about a customer that did not dial 911, a recently enacted exception to the ECPA’s^{12/} general prohibition on carrier disclosure of subscriber records or other information pertaining to electronic communications allows carriers to make available location information when the “provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.”^{13/} The problem with Petitioners’ argument that “[i]t makes little sense to differentiate the disclosure of customer information based on whether

^{9/} H.R. Rep. No. 106-25 at 7 (1999). This information may not be used for any other purpose unless the carrier receives the express “approval of the customer.” 47 U.S.C. § 222(c)(1).

^{10/} CTIA at 7; *see also DOJ Memo* at 6.

^{11/} *DOJ Memo* at 7-8 (“It is hard to imagine any clearer indication of the absence of an expectation of privacy than a cry for help; by reaching out to the government officials to seek their help, the caller indicates that he has no expectation of privacy in information that could help the authorities respond to the emergency.”); *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (citations omitted) (the Fourth Amendment is invoked when the person invoking its protection is able to “claim a ‘justifiable,’ a ‘reasonable,’ or a ‘legitimate expectation of privacy’ that has been invaded by government action. . .”).

^{12/} 18 U.S.C. § 2702(b), (c) (added respectively by the Homeland Security Act of 2002 and the USA Patriot Act of 2001).

^{13/} 18 U.S.C. §§ 2702(a)-(b), 2703(a)-(c); 18 U.S.C. § 2702(b)(8); *see also* 18 U.S.C. § 2702(c)(4) (“A provider . . . may knowingly divulge a record . . . to a government entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious personal injury to any person justifies disclosure of the information.”).

property or lives may be at risk”^{14/} is that Congress made exactly that distinction in sections 2702(b) and (c).^{15/} The law is clear on its face and there is simply no basis for granting Petitioners’ proposal to interpret the statutes in a manner that conflicts directly with their plain language.^{16/}

Even if the statutes were ambiguous, Petitioners’ arguments in favor of expanded disclosure is not supported by the legislative history. In adding section 222(d)(4) to the Communications Act in 1999, Congress explicitly recognized that the Commission already had ordered wireless carriers to provide Phase I and Phase II 911 location information to requesting PSAPs.^{17/} Section 222(d)(4) simply endorsed the DOJ’s previous finding that if a customer calls 911 and triggers the government’s emergency response, he impliedly consents to (and presumably wants) his location information to be disclosed. Similarly, the legislative history of sections 2702(b) and (c) makes clear that these narrow amendments were intended solely to provide carriers and law enforcement officials greater flexibility when dealing with especially

^{14/} *Petition* at 5.

^{15/} As CTIA explains, it is hard to argue that Congress is unaware of the grave effects that emergencies involving property impose on the public, especially in light of September 11th. Because Congress “nonetheless kept the exception for emergency disclosure narrow speaks volumes about Congressional intent even if the words ‘death or serious physical injury’ could somehow be read to be ambiguous.” CTIA at 10.

^{16/} *See also* Massachusetts Statewide Emergency Telecommunications Board (“MSETB”) at 2-3 (urging the Commission to expand the definition of the word user to allow carriers to release subscriber information regardless of whether the subscriber is the person making the call to 911).

^{17/} H.R. Rep. No. 106-25 at 7 (1999) (acknowledging that in 1997 the FCC had ordered wireless carriers to deliver location information about callers to 911 to the PSAP). Under the Commission’s E911 rules carriers are required to supply PSAPs with necessary information to allow the PSAP to locate the mobile phone user during emergency situations. 47 C.F.R. § 20.18(b) (licensees must transmit all “wireless calls . . . initiated by a wireless user dialing 911 on a phone”) (internal quotations omitted).

serious emergencies.^{18/} As Senator Leahy explained, “[i]n those cases where the risk of death or injury is imminent, the law should not require providers to sit idly by.”^{19/}

CTIA is correct, therefore, that the civil and criminal privacy statutes are not inconsistent.^{20/} Section 222(d)(4) allows carriers to comply with the Commission’s E911 rules when their customers call 911 regardless of the nature of the emergency, and sections 2702(b) and (c) cover circumstances in which the customer has not consented to the disclosure – either directly or impliedly by dialing 911 – but the danger is so severe and immediate that it outweighs the customer’s general privacy expectations. In all other situations, the carrier must first obtain the customer’s consent, a warrant, or a court order before disclosing location information.

Given that there is little ambiguity in either the statutory language or the congressional intent evidenced in the legislative history, it would not be appropriate for the Commission to grant Petitioners’ request to expand the scope of the statutes. Indeed, insofar as Petitioners ask the Commission to interpret the *criminal* code, such action would be outside the scope of the Commission’s responsibilities under the Communications Act.^{21/} Likewise, as Sprint explains, the Commission’s discretion to interpret its own authorizing statute is not unfettered -- “if the intent of Congress is clear, that is the end of the matter . . . [and] the agency, must give effect to

^{18/} See, e.g., 148 CONG. REC. 8901, S8901-02 (daily ed. Sept. 19, 2002) (statement of Sen. Hatch) (explaining that the amendment in the Homeland Security Act “creates a ‘good faith’ exception to allow communications providers to disclose communications to a governmental entity – e.g., hospital, law enforcement – in an emergency situation involving danger of death” and indicating that Congress still intended to address the “privacy concerns” associated with the amendment).

^{19/} 147 CONG. REC. 10990, S10999 (daily ed. Oct. 25, 2001) (statements of Sen. Leahy).

^{20/} CTIA at 7 (“Section 222 of the Communications Act is perfectly congruent with [the] ECPA on this score.”).

^{21/} CTIA at 10 (“the Commission lacks authority to modify [the] ECPA”); Sprint at 7 (“the Commission does not possess the statutory authority to rewrite the nation’s criminal laws.”).

the unambiguously expressed intent of Congress.”^{22/} AWS is fully committed to assisting its customers and PSAPs in emergencies and will continue to take all actions necessary – and consistent with the law – in fulfillment of this duty. At this point, however, Congress has drawn a clear line between when disclosure of confidential information is allowed and when it is not, and only Congress can give the Commission authority to move that line.^{23/}

II. THE COMMISSION SHOULD NOT FURTHER NARROW THE SCOPE OF ITS INTERPRETATION OF SECTION 222 OF THE COMMUNICATIONS ACT

In contrast to Petitioners, EPIC contends that section 222(d)(4) fails to protect adequately the privacy of consumers and, thus, it asks the Commission to place additional limitations on the disclosure of customer location information during emergency situations. In particular, EPIC argues that section 222(d)(4) should be interpreted to require “a caller’s consent before his location information can be disclosed when that caller does not personally require emergency services.”^{24/} Because EPIC’s proposal would be impossible to implement in today’s E911 environment, and because it is unnecessary to safeguard the privacy interests of consumers, EPIC’s request should be rejected.

EPIC apparently is unfamiliar with the Commission’s rules, and the technology that has been deployed, that require carriers to provide to the relevant PSAP the telephone number and location information associated with *every* caller to 911.^{25/} As a matter of law and technology, once Phase I or Phase II E911 service has been implemented in a market, the location of all

^{22/} Sprint at 9, quoting *Chevron USA v. Natural Resources Defense Council*, 467 U.S. 837, 842-43 (1984).

^{23/} AWS agrees with Sprint, however, that further clarification of carriers’ privacy obligations under the Communications Act and the ECPA would be helpful and, therefore, it supports Sprint’s suggestion that the DOJ provide a memorandum addressing the issues. Sprint at 3.

^{24/} EPIC at 2.

^{25/} 47 C.F.R. § 20.18.

callers to 911 is *automatically* transmitted to the PSAP. There is no mechanism built into the system to halt the process so that carriers or dispatchers can ask the caller if “he consents to location disclosure.”^{26/}

Nor would it be in the public interest to require carriers to delay delivery of the caller’s geographic coordinates to give PSAPs the opportunity to inquire of each person that has dialed 911 whether he is calling on behalf of another party and, if so, whether he wants his location to be disclosed. Not only is EPIC wrong that “[l]imiting disclosure of location information to users who personally require emergency assistance could increase response times in [an] emergency,” the exact opposite is true.^{27/} Attempting to distinguish between callers that need assistance themselves and those that are calling 911 for someone else, and then obtaining consent from the latter on a “case-by-case basis”^{28/} would slow response times to a crawl for *all* wireless 911 callers. This would conflict with, and fatally undermine, the very purpose underlying adoption of the Phase I and Phase II E911 requirements – saving lives. Because the need for prompt delivery of location information in an emergency far outweighs any interest a “good samaritan” 911 caller might have in withholding information about his own whereabouts, EPIC’s request should be rejected.

^{26/} EPIC at 2.

^{27/} EPIC at 2.

^{28/} EPIC at 3.

CONCLUSION

For the foregoing reasons, the Commission should deny both the Petitioners' request to expand the scope of the statutory disclosure requirements, and EPIC's proposed requirement that consent for CPNI disclosure must be obtained when a caller dials 911 on behalf of someone else.

Respectfully submitted,

AT&T WIRELESS SERVICES, INC.

Howard J. Symons
Sara F. Leibman
Susan F. Duarte
Mintz, Levin, Cohn, Ferris, Glovsky
and Popeo, P.C.
701 Pennsylvania Avenue, N.W.
Suite 900
Washington, D.C. 20004
Telephone: (202) 434-7300
Fax: (202) 434-7400

Of Counsel

Dated: September 15, 2003

/s/ Douglas I. Brandon

Douglas I. Brandon
Vice President - External Affairs
1150 Connecticut Avenue, N.W.
Suite 400
Washington, D.C. 20036
(202) 223-9222

CERTIFICATE OF SERVICE

I, Susan F. Duarte, hereby certify that on this 15th day of September 2003, the foregoing "Reply Comments of AT&T Wireless Services, Inc." were filed electronically on the FCC's Electronic Comment Filing System and copies were served by the method indicated on the following:

James R. Hobson
Miller & Van Eaton, P.L.L.C.
1155 Connecticut Avenue, N.W., Suite 1000
Washington, D.C. 20036
Counsel for NENA and NASNA

Via First Class Mail

Qualex International
Portals II
445 12th Street, S.W. Room CY-B402
Washington, D.C. 20554
qualexint@aol.com

Via Electronic Mail

Michael F. Altschul
Cellular Telecommunications
& Internet Association
1250 Connecticut Avenue, N.W.
Suite 800
Washington, DC 20036

Via First Class Mail

Susan M. Prosnitz
Statewide Emergency Telecommunications
Board
Executive Office of Public Safety
One Ashburton Place
Boston, MA 02108

Via First Class Mail

Robert M. Gurs
Fletcher, Heald & Hildreth PLC
1300 N. 17th Street
11th Floor
Arlington, Virginia 22209
Counsel for APCO

Via First Class Mail

David L. Sobel
Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009

Via First Class Mail

Luisa L. Lancetti
Vice President, PCS Regulatory Affairs
Sprint Corporation
401 9th Street, N.W.
Suite 400
Washington, DC 20004

Via First Class Mail

Brian Millen
Consumer and Governmental Affairs Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554
bmillen@fcc.gov

Via Electronic Mail

/s/ Susan F. Duarte
Susan F. Duarte