FEDERAL COMMUNICATIONS COMMISSION
Wireless E911 Location Accuracy Requirements; E911 Requirements for IP-Enabled Service Providers
PS Docket No. 07-114; WC Docket No. 05-196

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published June 20, 2007, the Federal Communications Commission ("FCC" or "Commission") filed a Notice of Proposed Rule Making ("NPRM") seeking comments on the Commission's proposed Enhanced 911 ("E911") rules.[1] Pursuant to that notice the Electronic Privacy Information Center ("EPIC") submits these Comments to inform the Commission that (1) the FCC has an obligation to protect the privacy of consumer information generated by the provision of communication services; (2) current regulations do not adequately location-based information, (3) legal frameworks, notably in the European Union, provide safeguards for location data, and (4) the Commission should establish rules that limit the use of customer location-based information. EPIC is a non-profit research and educational organization that examines the privacy and civil liberties implications of emerging technologies.

I. Introduction.

Under current law, section 222 of the Communications Act protects location information along with other Costumer Proprietary Network Information (CPNI), requiring user "approval" for uses or disclosures.[2] Further, "express prior authorization" of the customer is required for uses and disclosures of "call location" information, with certain exceptions.[3] These exceptions are to providers of emergency services, family and guardians in emergency situations, and information or database services solely for assisting in delivering emergency services.[4] The Commission has stated that this is an unambiguous requirement that a costumer "explicitly articulate approval" before a carrier may use location information.[5]

Both enacted and proposed E911 requirements should take into account the privacy considerations of location information. Several location-based services exist using location technologies.[6] The development of location-based services has been

---

[1] Wireless E911 Location Accuracy Requirements; E911 Requirements for IP-Enabled Service Providers, 72 Fed. Reg. 33,948 (June 20, 2007) [hereinafter E911 Notice].
[2] 47 U.S.C. § 222(c)(1).
[3] 47 U.S.C. § 222(f).
[4] 47 U.S.C. § 222(d)(4).
[5] *In the Matter of Request by the Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices*, Order, WT Docket No. 01-72, at 3 (July 24, 2002) *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-208A1.pdf.
[6] *See, e.g.,* Sprint Family Locator, https://sfl.sprintpcs.com/finder-sprint-family/signIn.htm; Ask Mobile, http://gps.ask.com/; Helio Buddy Beacon, http://www.helio.com/#services_gps.

spurred by E911 requirements.[7] EPIC supports the public safety and emergency services goals of the E911 project. At the same time, the misuse of location-based information could facilitate stalking and other criminal conduct. In this regard, the privacy interests in location-based information may be greater than any other personal information generated by the communications system because it would provide the physical location of a telephone customer in real time to someone who may intend to harm the customer. [8] Because of the further uses of location information that E911 creates, the Commission should take care that privacy and safety of location information also keeps up with its important location requirements.

In the current proceeding, the Commission asks for comments to update the record in the VOIP 911 proceeding.[9] In a previous NPRM as part of the VOIP 911 proceedings, the Commission asked whether the commission should "adopt any privacy protections related to provision of E911 service by interconnected VOIP providers."[10] Further, Commissioner Adelstein asks whether given improved accuracy the Commission should be taking a closer look at how privacy interests intersect with innovation in the E911 space.[11]

EPIC therefore files these comments to inform the Commission of the state of privacy protection for location information. Described herein are some inadequacies of current location privacy protection and some principles that should inform location privacy considerations. EPIC then addresses how these privacy considerations can address some of the Commissions specific requests in this rulemaking.

II. Current and Proposed CPNI Regulations Do Not Adequately Protect Location Information.

---

[7] Anne Chen, *After Slow Start, Location-Based Services Are on the Map*, eWeek.com, July 12, 2005, http://www.eweek.com/article2/0,1895,1621409,00.asp.

[8] *See e.g.* Marie Tessier, *Hi-Tech Stalking Devices Extend Abusers' Reach*, Women's E News, Oct. 10, 2006, http://www.womensenews.org/article.cfm/dyn/aid/2905/context/cover/ (describing two convicted stalkers: a Washington stalker that hid a GPS enabled telephone on his victim's automobile and an Arizona stalker that planted a GPS device); David Teather, *Man Arrested Over GPS 'Stalking,'* The Guardian, Sept. 6, 2004, http://www.guardian.co.uk/mobile/article/0,2763,1297893,00.html (a California man followed his victim after planting a GPS enabled cellphone in his victim's car);
Stalkers Use GPS to Track Victims, CastleCops, Feb. 7, 2003,
http://www.castlecops.com/modules.php?name=News&file=print&sid=2102 (a Wisconsin man stalked his victim by planting a GPS device in her car).

[9] *In the Matter of Wireless E911 Location Accuracy Requirements; Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems; Association of Public-Safety Communications Officials-International, Inc. Request for Declaratory Ruling; 911 Requirements for IP-Enabled Service Providers*, Notice of Proposed Rulemaking, PS Docket No. 07-114, CC Docket No. 94-102, WC Docket No. 05-196, at 7 (May 31, 2007) *available at*
http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-108A1.pdf [hereinafter E911 NPRM].

[10] *In the Matters of IP-Enabled Services; E911 Requirements for IP-Enabled Service Providers*, First Report and Order and Notice of Proposed Rulemaking, WC Docket No. 04-36, WC Docket No. 05-196, at 34-35 (May 19, 2005) *available at* http://www.fcc.gov/cgb/voip911order.pdf [hereinafter VOIP 911 Order].

[11] E911 NPRM, *supra* note 9 at 28.

Recent CPNI rulemaking responds to the problem of "pretexting."[12] EPIC, as part of a consumer coalition, separately filed comments in that matter.[13] As a result of the well founded concern with pretexting, the FCC adopted an important rule that protects CPNI, but the CPNI rules only incidentally protect specific consumer interests in location information.

Carriers face certain authentication requirements, though these are not adequately tailored to the protection of location information. Carriers may release call detail CPNI with costumer use of a password, by mailing to the address on record, or by calling the number on record.[14] Carriers may disclose non-call detail after authenticating the costumer, but no specific password or other system is required.[15] High authentication requirements are required to adequately protect location information. The Commission has separately requested comments on further extending these authentication requirements[16] and these may come to adequately protect the authentication of costumers with respect to their location information.

Carriers must notify consumers of certain account changes.[17] However, these changes do not include any of the costumer's preferences concerning location information privacy. Nor, more generally, the "approval" for uses and disclosures of CPNI that § 222 requires.

Consumers are not adequately notified of unauthorized uses of their location information. Carriers must first notify law enforcement of CPNI breaches.[18] Law enforcement may postpone notification to the consumer.[19] Carriers may notify consumers after consultation if they believe that there is an extraordinarily urgent need to avoid immediate and irreparable harm.[20] Breaches of location information may lead to situations of such serious harm, but the carrier has no method of determining for each case the danger posed. The consumer, on the other hand, does.

Consumer control over location information is not adequately protected by current CPNI regulation. Carriers must obtain opt-in consent before disclosing CPNI to joint

---

[12] *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carrier's Use of Costumer Proprietary Network Information and Other Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115, WC Docket No. 04-36, at 2 (March 13, 2007) *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf [hereinafter CPNI Report, Order & NPRM].

[13] Comments of the Consumer Coalition, *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carrier's Use of Costumer Proprietary Network Information and Other Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36 (July 9, 2007) *available at* http://www.epic.org/privacy/cpni/cpni_070607.pdf.

[14] CPNI Report, Order & NPRM, *supra* note 12 at 10-11.

[15] *Id.*

[16] CPNI Report, Order & NPRM, *supra* note 12 at 36.

[17] *Id.* at 17.

[18] *Id.* at 19.

[19] *Id.*

[20] *Id.*

venture partners or independent contractors.[21] Per § 222, carriers are already required to seek "express prior authorization" for use, disclosure and access to call location information.[22] However, the collection and retention of location information is not covered by this rule or statute. Carrier use and retention of location information besides call location information is also not addressed.

Several of the other proposed CPNI rules may come to protect location information privacy even though that was not their focus. The Commission requested comments on the use of audit trails, physical safeguards and limits on data retention.[23] However, given the Commission's and thus commenter's concern with pretexting, it is likely that such protection will also be incidental.

III. Towards Adequate Location Information Privacy.

An adequate location privacy regime will contain several features not currently addressed by CPNI regulations. The European location privacy regime is useful for highlighting these. Two other principles -- technology neutrality and technology pacing -- are of special concern in an area where mandates are driving technological development among a variety of technologies choices.

The EU Directive on Privacy and Electronic Communications, adopted in 2002, addresses cellular location information.[24] The Directive provides the basis for communications privacy for the 27 members of the European Union. The EU Directive differentiates between location information needed to enable transmission and more accurate location information used for value added services.[25]. Location data other than traffic data is treated under Article 9.[26] Article 9 requires that location data be processed anonymously or with consent.[27] Obtaining this consent requires informing the user of the type of data, the purpose of the collection, the duration of the collection and whether a third party will be doing the processing.[28] Consent may be withdrawn at any time.[29] There must be a simple and free means for a subscriber to refuse the processing of location data for a specific connection or transmission.[30] Transmission of data may only be made to those providing the value added service.[31] The processing of data is limited to what is necessary for providing the value added service.[32]

---

[21] *Id.* at 22.
[22] 47 U.S.C. § 222(f)
[23] CPNI Report, Order & NPRM, *supra* note 12 at 36-37.
[24] Directive on Privacy and Electronic Communications 2002/58, 2002 O.J. (L 201) 37, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.
[25] *Id.* at ¶ 35, 41.
[26] *Id.* at art. 9, 45.
[27] *Id.* at art. 9(1), 45.
[28] *Id.*
[29] *Id.*
[30] *Id.* at art. 9(2), 45.
[31] *Id.* at art. 9(3), 45.
[32] *Id.*

The Article 29 Working Party, made up of the Data Protection Commissioners from the EU, has issued an opinion addressing location information that could further guide the development of appropriate regulations to safeguard location information.[33] "Consent" is to mean specific consent, not obtained as part of agreement to general terms.[34] The Working Party notes that when third parties are involved in providing location based services, protection can be achieved by configuring the technology in such a way that the third party is not aware of the identity of the individual.[35] Another method to minimize the data transfer is to move as much of the processing of data to the individual handset as made possible by increasing network bandwidth, handset processing and storage capacities.[36] The opinion gives the example of where an individual downloads a listing of restaurants in a city from a third party, and thus can this listing based on their location without transmitting their location to a third party service provider.[37]

The Article 29 Working Party opinion recommends that measures should be taken to ensure that consent is valid.[38] A notice of subscription to a location service should be sent to the handset.[39] If necessary, the provider should request confirmation of the subscription.[40] This is akin to the system used by some electronic mailing lists of a "double opt-in."[41] These steps help to prevent fraudulent subscription without the individual's knowledge.[42] In order to perfect them, the notice and reconfirmation should be sent with some delay, at a random time. For example, a journalist reported the ability to stalk his spouse by signing up her telephone for a location tracking service.[43] The service sent the confirmation and notice of signup immediately, negating its protection against unauthorized access to the device.[44] This vulnerability negates the need for the stalker to plant the device on the victim as described above.[45]

Several specific lessons are available from the European example which the Commission should draw from. First, location should receive special consideration above other traffic information. While section 222 addresses location specifically,[46] the

---

[33] Working Party 29 Opinion on the use of location data with a view to providing value-added services, 2130/05/EN (Nov. 2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf [hereinafter Working Party Opinion].
[34] *Id.* at 5.
[35] *Id.* at 6.
[36] *Id.*
[37] *Id.*
[38] *Id.* at 6.
[39] *Id.*
[40] *Id.*
[41] *See* Double Opt-In, http://email.about.com/library/glossary/bldef_double_opt-in.htm.
[42] Working Party Opinion*, supra* note 33 at 7.
[43] Ben Goldacre, *How I Stalked My Girlfriend,* The Guardian, Feb. 1, 2006, http://www.guardian.co.uk/technology/2006/feb/01/news.g2.
[44] *Id.*
[45] *See supra* note 8.
[46] 47 U.S.C. § 222(f).

Commission has not issued any location privacy rules. Second, consent and individual control should be properly authenticated and available at a fine grain.

Sensible protection of location privacy should be technology neutral. Various devices and services will make use of location data in different ways,[47] but consumers will have consistent, commonsense privacy expectations. Consumers should not have to find that when they use a different technology, or use a given technology differently, they are endangering their privacy. Furthermore, privacy threats may be technology specific, as different technologies may be susceptible to different security attacks. Different services or uses of services may require different configuration of information flows. The protection against these varied threats should be the responsibility of the providers that have designed and chosen these technological configurations. Consumers should be able to expect similar privacy throughout their uses of various devices and services.

Lastly, to adequately protect location privacy, the level of privacy protection should pace location technology. Privacy protections should increase in response to increasing accuracy of location technology. The goal of increasing accuracy standards is public safety and better emergency response.[48] Consumers should not have to be concerned that their privacy is exposed by accuracy mandates meant to promote their safety. Consumers should not be forced to choose between privacy protection and safer, more accurate E911 location information. Safer and more accurate location technologies will be adopted faster and welcomed by consumers if consummate privacy protections are enacted. The appropriate response to public safety accuracy increases is to increase privacy protection accordingly.

IV. Addressing Specific Items of the FCC rulemaking.

With the above concerns in mind, EPIC addresses some of the specific items of the Commission's rulemaking.

a. How advances in technologies and use of hybrid technologies should impact analysis.

The Commission should keep aware of technology pacing and technology neutrality when considering advances in technologies. The Commission should take care that different technologies do not create different privacy intrusions which consumers are expected to be aware of. Further, the Commission should make sure that accuracy advances do not outstrip the privacy protections afforded to location data.

b. Whether more stringent accuracy requirement should be adopted.

The Commission should adopt more stringent accuracy requirements only after taking into account the adequacy of location privacy protection. The admirable goal of

[47] *See supra* note 6.
[48] E911 NPRM, *supra* note 9 at 1;

emergency response is driving the industry for location-based services.[49] In meeting this goal, the Commission also has a responsibility to protect consumer privacy.[50]

c. How and by what date to require compliance with new accuracy requirement.

As above, the Commission should keep in mind the principle of technology pacing. EPIC recommends that compliance timeframes permit the development of adequate privacy safeguards for location information.

d. Extension of E911 requirements to VOIP.

Along with the principle of technology neutrality, the Commission should take care that VOIP providers are delivering the same level of privacy protection to location information that other services do. In its extension of CPNI rules to VOIP technologies, the Commission concluded that it "seems reasonable for American consumers to expect that their telephone calls are private irrespective of whether the call is made using the services of a wireline carrier, a wireless carrier, or an interconnected VOIP provider, given that these services, from the perspective of a customer making an ordinary telephone call, are virtually indistinguishable."[51] At a minimum, the Commission should ensure that E911 requirements follow CPNI requirements. Specifically, the Commission should take care that the legal arguments that form the basis of the E911 application to VOIP are comparable to those that apply to CPNI, so that those two claims of ancillary jurisdiction rise and fall together. If VOIP CPNI requirements are withdrawn or overturned for any reason, the Commission should do the same for E911.

Further, the Commission should take care that the specific technologies involved with VOIP do not raise location privacy concerns which are beyond the current CPNI mandates, or beyond the Commission's regulatory reach. VOIP technologies may have different security issues than connections that are made via the wire or wireless networks. End user terminals may have different software configurations, and may run applications on top of third party software with its own security problems. These security and privacy issues may depend on circumstances, services and technologies which the Commission does not currently regulate. If the Commission does not notice and correct these, the principle of technology neutrality would be violated. This would leave consumers exposed to different privacy protections and unreasonably tasked with research the regulatory regime that their devices are under.

V. Conclusion

The generation of location information for emergency services raises important privacy and personal safety concerns that the Commission should address. The

[49] Chen, *supra* note 7.
[50] 47 U.S.C. § 222.
[51] CPNI Report, Order & NPRM, *supra* note 12 at 31.

Commission has a statutory obligation to develop rules to ensure that personal information collected for an appropriate purpose is not misused or subjects telephone customers to personal risk.

Respectfully submitted,

Marc Rotenberg
Executive Director

Guilherme Roschke
Skadden Fellow

Evan Stern
EPIC IPIOP Clerk

Ravinder Singh
EPIC IPIOP Clerk

Electronic Privacy Information Center
1718 Connecticut Ave NW, #200
Washington DC, 20009
www.epic.org
202-483-1140 (tel)
202-483-1248 (fax)

August 10, 2007