Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of Wireless E911 Location Accuracy Requirements	PS Docket No. 07-114

COMMENTS OF
PUBLIC KNOWLEDGE
ALVARO BEDOYA
AMERICAN CIVIL LIBERTIES UNION
BENTON FOUNDATION
CENTER FOR DEMOCRACY & TECHNOLOGY
CENTER FOR DIGITAL DEMOCRACY
COMMON SENSE MEDIA
CONSUMER ACTION
CONSUMER FEDERATION OF AMERICA
CONSUMER FEDERATION OF CALIFORNIA
CONSUMER WATCHDOG
ELECTRONIC FRONTIER FOUNDATION
ELECTRONIC PRIVACY INFORMATION CENTER
NEW AMERICA FOUNDATION'S OPEN TECHNOLOGY INSTITUTE
PRIVACY RIGHTS CLEARINGHOUSE
U.S. PIRG
WORLD PRIVACY FORUM

Laura Moy
Public Knowledge
1818 N St, NW
Suite 410
Washington, DC 20036
(202) 861-0020

Filed December 15, 2014

For Commenters

Table of Contents

Summary

Public Knowledge, Alvaro Bedoya,[1] American Civil Liberties Union, Benton Foundation,[2] Center for Democracy & Technology, Center for Digital Democracy, Common Sense Media, Consumer Action, Consumer Federation of America, Consumer Federation of California, Consumer Watchdog, Electronic Frontier Foundation, Electronic Privacy Information Center,[3] New America Foundation's Open Technology Institute, Privacy Rights Clearinghouse, U.S. PIRG, and World Privacy Forum (collectively "privacy advocates") respectfully respond to the FCC's request for comments regarding the location accuracy "roadmap" submitted by the Association of Public Safety Communications Officials ("APCO"), the National Emergency Number Association ("NENA"),

[1] Center on Privacy and Technology at Georgetown Law (affiliation provided for identification purposes only).

[2] The Benton Foundation is a nonprofit organization dedicated to promoting communication in the public interest. These comments reflect the institutional view of the Foundation and, unless obvious from the text, are not intended to reflect the views of individual Foundation officers, directors, or advisors.

[3] Privacy in the E911 context is a longstanding issue for the Electronic Privacy Information Center. *See Wireless E911 Location Accuracy Requirements*, Docket No. PS 07-144, Comments of the Electronic Privacy Information Center (filed Aug. 10, 2007), *available at* https://epic.org/privacy/pdf/EPIC_e911_Comments.pdf.

and the four national wireless carriers.[4] The roadmap raises significant privacy-related concerns that are not adequately addressed in the roadmap itself. In light of these newly raised concerns, privacy advocates urge the Commission to pass regulations that require commercial mobile radio service ("CMRS") carriers and others to treat mobile 911 location information and National Emergency Address Database ("NEAD") as protected information, to require that representatives of consumer privacy organizations be allowed to participate fully in the further development of improved E911 location accuracy, and to ensure that any final agreement(s) will be subject to further notice and comment.

In the event the Commission moves forward with an Order in this docket and determines that the record is currently insufficient to support the regulations that privacy advocates recommend, the Commission should issue a Further Notice of Proposed Rulemaking proposing privacy regulations for wireless E911 location data.

I. The Roadmap Raises Privacy Concerns

The roadmap raises a number of privacy concerns. These concerns relate to the design and implementation of the NEAD, the deployment of "beacon" technology, and whether and how location information derived from these technologies will be protected under FCC regulations.

A. The Proposed "National Emergency Address Database" Would Contain Sensitive Information

First, the proposed establishment and existence of the NEAD is deeply concerning because NEAD would collect and retain sensitive information. According to the roadmap, "[t]he NEAD is the database that provides the correlation between MAC address [of each beacon] and dispatchable location." A MAC address is a unique identifier for a device. For example, suppose a wi-fi

[4] *See* Letter from John Wright, APCO International, *et al.*, to Marlene Dortch, Secretary, FCC (Nov. 18, 2014), *available at* http://apps.fcc.gov/ecfs/comment/view?id=60000983188 [hereinafter Roadmap].

router at Public Knowledge had the address 1a:2b:3c:4e:5f:6a. The corresponding line in NEAD might look like this:

MAC Address	Street 1	Street 2	City	State
1a:2b:3c:4e:5f:6a	1818 N St, NW	Suite 410	Washington	DC

This information is sensitive for at least three reasons. First, users of networked devices likely do not expect that information about their device and physical address will be stored in a national database that is accessible to multiple parties. Second, as the database is updated over time, it could reveal the exact address of individuals who have moved from one location to another and brought their networked devices with them. Third, software vulnerabilities make it possible for malicious third parties to obtain their victims' MAC addresses remotely, which—with access to a database like NEAD—could then be used to derive physical address as well.[5]

Because of these concerns and others, companies that catalog MAC addresses in databases similar to NEAD have provided consumers with an opt-out. For example, Google allows consumers to opt out of having their devices included in the Google Location Service by appending "_nomap" to their SSID.[6] Yet the roadmap mentions neither an opt-in nor opt-out for wireless device owners who do not wish their devices to be included in a new national database.

---

[5] *DD-WRT, I Know Where You Live*, /DEV/TTYS0, (Dec. 27, 2001), http://www.devttys0.com/2010/12/dd-wrt-i-know-where-you-live/. In response to revelations regarding privacy concerns and MAC address databases, Microsoft and Google both instituted new privacy protections. Similar protections are nowhere to be found in the Roadmap. *See* Peter Bright, *Microsoft Locks Down Wi-Fi Geolocation Service After Privacy Concerns*, Ars Technica (Aug. 2, 2011), http://arstechnica.com/information-technology/2011/08/microsoft-locks-down-wi-fi-location-service-after-privacy-concerns/.

[6] *Configure Access Points with Google Location Service*, Google (last visited Dec. 8, 2014), https://support.google.com/maps/answer/1725632?hl=en.

B. There Is No Indication that Signatories Will Adhere to Critical Safeguards for Sensitive Information in NEAD

Not only will the information contained in NEAD be sensitive, the *use* of NEAD will also be sensitive because it will facilitate highly accurate location technology, but the roadmap provides no assurance of critical safeguards. For example, there is no indication that the database will be secure, used only for E911 purposes, and never sold to or otherwise shared with third parties, including government entities. The roadmap states simply that the signatories will work together "to develop the design, operations, and maintenance requirements" and "to establish a database owner, funding mechanisms, provisions for defining security/privacy, performance, and management aspects."[7]

C. The Deployment of "Beacon" Technology Described in the Roadmap Raises Concerns

The deployment of beacon technology, as described in the roadmap, also raises concerns. To develop the capability to deliver location results with the high degree of precision required by the Commission's proposed rules, signatories will need to ensure that beacons are placed sufficiently densely on a national scale. To accomplish this, the signatories propose both to deploy their own devices to serve as beacons, and to work with third parties to build out the network. The roadmap states,

> To the extent that a carrier plans to introduce new wireless consumer home products, such carrier agrees to introduce such products that will provide dispatchable location . . . . Products not installed by carrier representatives may require the customer to

[7] Roadmap at 5.

> input dispatchable location data (e.g., apartment number) into the product or device.[8]

The roadmap also states,

> [The signatories] agree to work together at the federal, state, and local level to develop an outreach program that will promote a broader integration of a variety of dispatchable location sources into the NEAD, and enlist the support of other organizations (e.g., hotel associations) to achieve this goal.[9]

It may seem natural to expand the number and density of beacons in order to improve location accuracy of E911 services, but any efforts to expand beacon infrastructure in this manner must take into consideration other possible uses of the infrastructure, some of which threaten consumer privacy. Once new beacons are deployed, they may be used to improve location accuracy not only of E911 services, but also of other services, including commercial services, that rely on the same technology. This is concerning because consumers are highly protective of information about their location. For example, according to a report released last month by the Pew Research Center, 82% of American adults considered the details of their physical location gathered over a period of time from the GPS on a cell phone to be "very sensitive" or "somewhat sensitive."[10] And a national survey conducted earlier this year by Anzalone Liszt Grove

[8] Roadmap at 4.
[9] Roadmap at 5.
[10] 50% said this information is "very sensitive"; 32% said it was "somewhat sensitive. Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* 34 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

Research found that "Americans overwhelmingly support proposals to limit corporate surveillance."[11]

The proposed methods to expand beacon infrastructure raise additional concerns. For example, requiring consumers to input dispatchable location information specific to the level of apartment number could violate consumers' expectations of privacy. It could also generate new stores of sensitive customer information that will have to be appropriately safeguarded by carriers.

The "broader integration of a variety of dispatchable location sources into the NEAD" also raises concerns. There are a number of companies across the country that are building out wi-fi and Bluetooth networks and beacons of their own, and the signatories aim to collect information about many disparate networks into one massive database. As mentioned above, the mere existence of that database presents new problems for data security and third-party sharing restrictions. But additionally, the integration proposal raises questions about incentives. How will the existence of NEAD alter the incentives of signatories and other parties considering whether to build out beacon infrastructure? To get third parties to contribute information about their networks to the NEAD and keep that information updated, what will the signatories offer in exchange?

D. It Is Not Clear Whether and How Existing Privacy Regulations Would Apply in the Context of the Roadmap

Finally, the roadmap raises a number of concerns and questions about how the FCC's privacy regulations will apply to location information derived from the described technologies. As new technologies are developed, questions arise about whether the information will be covered under the Commission's existing privacy framework. For example, the Commission's rules governing customer proprietary network information ("CPNI") would likely apply to location information collected by a customer's device via the described beacon

[11] *Americans Strongly Support Reining in Corporate Surveillance*, Anzalone Liszt Grove Research (Feb. 27, 2014), http://media.wix.com/ugd/c4876a_e2bb10a741804cd981e7c67e70488dad.pdf.

technology.[12] But this should be clarified, and the Commission must also determine what safeguards are appropriate for any information described in the roadmap that is not or may not be CPNI such as NEAD itself, which, as described, would contain large amounts of information about wi-fi and Bluetooth devices that do not belong to customers of a Title II service.

II. If These Concerns Are Not Addressed at This Stage, We May Lose Important Opportunities to Protect Privacy

The Commission must encourage privacy by design in the development of new technologies that respond to E911 improved location accuracy regulations. If the Commission does not incorporate privacy by design at this early stage, the anticipated privacy threats outlined above could come to pass, become entrenched, and be much more difficult to address in the future.

Indeed, this is what happened when the Commission passed the first rules to require mobile E911 location information. The technologies that became widespread as a result of those rules were exploited by third party companies in ways that consumers did not anticipate or agree with, and regulators have since struggled to prevent abuses of consumer location information.

In 1996, citing the growing use of mobile phones and the growing inability of emergency responders to locate callers in a timely fashion, the Commission issued new rules for wireless E911 mandating that carriers determine and transmit the location of 911 callers. As part of that process, CTIA, APCO, NENA, and the National Association of State Nine One One Administrators ("NASNA") agreed "within five years . . . to require deployment of [Automatic Location Identification ("ALI")] for wireless callers in two dimensions . . . within 125

[12] "[T]he definition of CPNI in section 222 and the obligations flowing from that definition apply to information that telecommunications carriers cause to be stored on their customers' devices when carriers or their designees have access to or control over that information." *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, 9611 (June 27, 2013) at ¶ 8.

meters."[13] The Consensus Agreement reached by the parties did not include any privacy provisions.[14] The Commission "sought comment on the necessity for, and implications of, imposing privacy requirements on information, such as name, address and telephone number, transmitted . . . in the delivery of 911 emergency services."[15] But no comments were filed by consumer privacy organizations, consumer privacy organizations do not appear to have been included in the development of the Consensus Agreement reached by CTIA, and the Commission did not seek comment on the privacy implications of the new technologies that would help carriers comply with heightened updated E911 regulations.

Within a few years, it became clear that the ALI technology mandated for customer safety purposes would be widely used for other purposes. A 1998 piece written for *Wireless Review* warned,

> Once wireless networks acquire the ability to locate users quickly and accurately during emergencies, they also will be able to track their every movement. Although this could prove a valuable tool for law enforcement agencies conducting legitimate criminal investigations, it opens the door to Big Brother–style abuses.[16]

And according to a 2000 piece in *InfoWorld*,

---

[13] Public Notice, Commission Seeks Additional Comment in Wireless Enhanced 911 Rulemaking Proceeding Regarding "Consensus Agreement" Between Wireless Industry Representatives and Public Safety Groups, CC Docket No. 94-102, DA 96-198, Feb. 16, 1996; 61 FR 6963 (Feb. 23, 1996) [hereinafter Consensus Agreement]; *see In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, Report and Order and Further Notice of Proposed Rulemaking (1996) at ¶ 11 [hereinafter 1996 R&O].

[14] *See* Consensus Agreement.

[15] 1996 R&O at p. 46.

[16] Ira Brodsky & Laurey Lummus, *Don't Look Now – You're Being Followed*, Wireless Review (Feb. 15, 1998) at 176.

> The ability to pinpoint the position of potential customers as they use their wireless phones is already a technical possibility, given systems developed for government emergencies and for 911 service.
>
> . . . .
>
> . . . [I]n limited trials, Xypoint, its partners, and a handful of other vendors are using ALI for commercial purposes. For now, they are doing so only with the express consent of a small number of wireless phone users.
>
> Go2Systems, in Irvine, Calif., is one of a swarm of vendors eyeing the use of ALI data. The company inked a five-year deal last week with Coca-Cola to steer wireless customers to stores selling Coke products. . . .
>
> Not limited to retail applications, m-commerce vendors are also ready to pitch ALI-related applications to enterprises needing to transmit corporate data to an increasingly mobile workforce.[17]

The summary report from a WAP-W3C joint workshop on mobile web privacy in 2000 remarked, "the E911 directive in the U.S. is well-intended, but may end up unwittingly leading to an infrastructure of mass tracking and surveillance."[18]

Indeed, one industry representative from XY Point Corporation, a provider of wireless location services, believed it was necessary to commercialize location information in order to pay for the new technology:

> So you have a [911] regulatory issue that is driving the wireless carriers under this obligation to move forward with the development of the [location] technology, and then you have the

---

[17] Jennifer Jones, *Vendors Walk Thin Line*, InfoWorld (Dec. 11, 2000) at 1–2.
[18] W3C and WAP, Report from WAP-W3C Joint Workshop on Mobile Web Privacy 7-8 December 2000, Munich, Germany, http://www.w3.org/P3P/mobile-privacy-ws/report.html

> commercial opportunity and the revenue opportunity that is driving it in other parts of the world, except at the same time you have U.S. carriers who are very much interested in trying to design applications that are going to pay for this regulatory obligation.[19]

By that time mobile location technology was already being developed and implemented, but regulators were seemingly just beginning to think about how to address the emerging privacy problems. In December 2000, the Federal Trade Commission held a workshop on *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*.[20] One of the five main topics of the workshop was privacy, and the report that followed the workshop noted that "[p]anelists generally agreed that the generation and potential use of location-based information is one of the most significant privacy issues in the wireless space."[21]

But because the regulatory structure covering mobile location information is incomplete or not vigorously enforced, and because self-regulation is inadequate to fully address consumers' privacy concerns, a decade later serious problems persist with the commercial use of mobile location information. According to the Pew Research Internet Project, as of September 2012 19% of all cell owners had turned off the location tracking feature on their cell phone because they were concerned that other individuals or companies could access

---

[19] Federal Trade Commission, Transcript of The Mobile Wireless Web, Data Services & Beyond: Emerging Technologies & Consumer Issues (2000), *available at* https://web.archive.org/web/20111105103130/http://ftc.gov/bcp/workshops/wireless/001212.htm.

[20] Federal Trade Commission, *Staff Report: Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues* (2002), http://www.ftc.gov/sites/default/files/documents/reports/mobile-wireless-web-data-services-and-beyond-emerging-technologies-and-consumer-issues/wirelesssummary_0.pdf.

[21] *Id.* at 8.

that information.[22] That number might be even higher if consumers had a better understanding of how mobile location information is used, but according to the Government Accountability Office,

> [B]ecause companies have not made clear and consistent disclosures about how they use and share location data, consumers may be unaware which third parties are using their location data (or that third parties are using it at all) and that law enforcement may obtain their location data and use it for surveillance. Furthermore, because consumers are expected to rely on these disclosures when judging whether they should give consent to a company to access their location, consumers may be providing such consent without complete knowledge of how their data will be used. . . . Consequently, users lack sufficient information to adequately judge whether they should trust those companies with their personal information.[23]

Moreover, more and more, mobile devices are used by teens and even children—users whose location might be considered more sensitive than adults', and who are less equipped to consider the implications of sharing location information with third parties.[24]

To prevent a similar outcome with respect to the improved location technologies that will be developed and implemented in response to the Commission's proposed E911 improved location accuracy rules, the Commission

---

[22] Pew Research Internet Project, *Privacy and Data Management on Mobile Devices* 2 (2012), http://www.pewinternet.org/2012/09/05/main-findings-7/.
[23] Government Accountability Office, *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy* 25 (2012), http://www.gao.gov/assets/650/648044.pdf.
[24] *See* Common Sense Media, *Zero to Eight: Children's Media Use in America 2013* (2013) (finding children's access to mobile media devices dramatically higher in 2013 compared to 2011), https://www.commonsensemedia.org/research/zero-to-eight-childrens-media-use-in-america-2013.

must take pains at this early stage to protect consumer privacy and foster a privacy-by-design approach to new location technologies.

III. The Commission Must Take Steps to Protect Privacy and Foster a Privacy-by-Design Approach

The Commission must take strong action now to ensure its rules for wireless location accuracy include a comprehensive framework to protect the location privacy of mobile devices, and to ensure that those designing technologies to respond to the new rules incorporate privacy by design. In particular, the Commission should pass regulations that require CMRS carriers and others to treat mobile 911 location information and NEAD as protected information and prohibit its sharing with third parties.[25] The Commission should also require that representatives of consumer privacy organizations be allowed to participate fully in the further development of improved E911 location accuracy as the Commission progresses in its development of E911 location accuracy rules. Finally, the Commission should preserve future opportunities to evaluate proposed solutions for privacy safeguards by ensuring that any final agreement(s) will be subject to further notice and comment.

The Commission should pass regulations to do the following:

- require carriers and others obligated to comply with improved E911 location accuracy requirements to treat location information derived from responsive technologies as CPNI
- require carriers and others obligated to comply with improved E911 location accuracy requirements to afford all entries in NEAD the same protections afforded to CPNI

[25] The Commission should also require the use of Privacy Enhancing Techniques, such as "differential privacy" and the assurance of "technological due process." *See* Cynthia Dwork, *Differential Privacy: A Survey of Results*, 1, 2008, http://www.cs.ucdavis.edu/~franklin/ecs289/2010/dwork_2008.pdf; Danielle Keats Citron, *Technological Due Process* (2008).

- require telecom carriers, cable operators, and satellite operators that offer wireless consumer home products to provide consumers who purchase or use such products to opt out of including their products in NEAD
- require carriers and others obligated to comply with improved E911 location accuracy requirements to ensure that location information and NEAD are secure

Simply by using their phones in a typical fashion, customers have no choice but to share massive amounts of rich personal information about themselves and their loved ones with the third parties who provide services. Customers expect that that information will be afforded strong protections, and that they will be given clear opportunities to provide or refuse consent for parties that wish to use sensitive information for other purposes.

The Commission possesses the necessary authority to pass these regulations under the § 201(b) just and reasonable standard, its § 222 authority governing CPNI, its §§ 303(b) and (r) authority to set service rules, its § 338 satellite privacy authority, and its § 551 cable privacy authority.

In the event the Commission determines that the record in this docket is currently insufficient to support the issuance of such regulations, the Commission should issue a Further Notice of Proposed Rulemaking to supplement the docket as necessary.

As APCO, NENA, carriers, and other interested parties continue to develop proposals for E911 location accuracy, the Commission should also require that representatives of consumer privacy organizations are invited and allowed to participate fully in discussions giving rise to any new agreements among the parties. Inclusion of consumer privacy representatives is key to a privacy-by-design approach.

The Commission should also preserve future opportunities for members of the public to weigh in on the signatories' plans as those plans develop. Privacy

advocates commend the Commission for putting the draft roadmap out on public notice at this early stage, but the roadmap lacks critical details concerning privacy. As privacy measures are developed (or fail to be developed) the Commission should continue to carefully consider each iteration of the signatories' plans, soliciting input from the public at each stage.

Conclusion

For the above stated reasons, the Commission should pass regulations that require CMRS carriers and others to treat mobile 911 location information and NEAD as protected information, require that representatives of consumer privacy organizations be allowed to participate fully in the further development of improved E911 location accuracy, and ensure that any final agreement(s) will be subject to further notice and comment.

Respectfully submitted,

Public Knowledge
Alvaro Bedoya
American Civil Liberties Union
Benton Foundation
Center for Democracy & Technology
Center for Digital Democracy
Common Sense Media
Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumer Watchdog
Electronic Frontier Foundation
Electronic Privacy Information Center
New America Foundation's Open Technology Institute
Privacy Rights Clearinghouse
U.S. PIRG
World Privacy Forum

By:

/s/

Laura Moy
Public Knowledge
1818 N St, NW
Suite 410
Washington, DC 20036
(202) 861-0020 ext. 106

Filed: December 15, 2014