January 22, 2015

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 12 St. SW
Washington, DC 20554

Re: PS Docket No. 07-114, *Wireless E911 Location Accuracy Requirements*

Dear Ms. Dortch:

Earlier this week, representatives from several privacy and consumer organizations (collectively "privacy advocates") had three meetings with staff of the Federal Communications Commission:

1. On Tuesday, January 20, Laura Moy of New America's Open Technology Institute, Adam Eisgrau of American Library Association, Alethea Lange of Center for Democracy & Technology, Chris Soghoian of American Civil Liberties Union, Harold Feld of Public Knowledge, Jeremy Gillula of Electronic Frontier Foundation, Susan Grant of Consumer Federation of America, Amina Fazlullah of Benton Foundation, and Linda Sherry of Consumer Action met with Gigi B. Sohn, Special Counsel for External Affairs and Daniel Alvarez, Legal Advisor to Chairman Tom Wheeler.

2. On Tuesday, January 20, Laura Moy of New America's Open Technology Institute, Jodie Griffin of Public Knowledge, Jeremy Gillula of Electronic Frontier Foundation, Susan Grant of Consumer Federation of America, Amina Fazlullah of Benton Foundation, and Rachel Levinson-Waldman of Brennan Center for Justice met with Louis Peraertz, Legal Advisor to Commissioner Mignon Clyburn.

3. On Wednesday, January 21, Laura Moy of New America's Open Technology Institute, Jodie Griffin of Public Knowledge, Jeremy Gillula of Electronic Frontier Foundation, Susan Grant of Consumer Federation of America, Chris Soghoian of American Civil Liberties Union, and Linda Sherry of Consumer Action met with Priscilla Argeris, Legal Advisor to Commissioner Jessica Rosenworcel.

In each meeting, privacy advocates reiterated points from the letter we sent to the Chairman and Commissioners on January 13, 2015.[1] Privacy advocates explained that the creation of rules that will require carriers to provide emergency responders with highly precise location information in the event of a 911 call will set in motion the development and deployment of technological solutions that raise a number of important privacy concerns. Privacy advocates explained that a number of those concerns are detailed in comments filed on December 15, 2014 by many of the organizations represented among privacy advocates, and others, in response to the FCC's request for comments regarding the roadmap submitted by the Association of Public Safety Communications Officials ("APCO"), the National Emergency Number Association ("NENA"), and the four national wireless carriers.[2]

Privacy advocates explained that it is critical for the Commission to address privacy concerns associated with E911 at this stage, before the technology is developed and deployed, so that entities that must comply with the E911 rules can plan the development and deployment of the necessary technology in accordance with privacy guidelines. It would be much more difficult to implement privacy safeguards after the technology has already been deployed.

Privacy advocates asked that an Order in the above-referenced docket enumerate and describe specific elements that carriers must include in their E911 privacy and security plans to be submitted to the FCC for certification.

---

[1] Letter from New America's Open Technology Institute, et al. to Chairman Wheeler and Commissioners, PS Docket. No. 07-114 (filed Jan. 13, 2015), *available at* http://apps.fcc.gov/ecfs/document/view?id=60001013237.
[2] Comments of Public Knowledge, et al., PS Docket No. 07-114 (filed Dec. 15, 2014), *available at* http://apps.fcc.gov/ecfs/document/view?id=60001009740.

Specifically, privacy advocates urged the Commission to require carriers to include the following elements in their privacy and security plans:

A mechanism whereby owners of wireless consumer home products are able to opt out of having their devices included in the National Emergency Address Database ("NEAD"). Privacy advocates explained that users of networked devices likely do not expect that information about their personal devices and physical address will be stored in a national database that is accessible to multiple parties, and should have the option not to include select devices in the database. Even private companies that collect information about wireless consumer home products provide consumers with the ability to opt out.[3] Privacy advocates also explained that it is unlikely that many consumers will opt out of NEAD if all privacy concerns are considered and addressed before the updated E911 system is deployed. Relatedly, privacy advocates also urged that the Commission require that NEAD only be used for 911 purposes and never be shared with third parties.

A system design in which E911 location functionality can only be triggered through the handset, and not remotely. Privacy advocates explained that because the updated E911 system will be capable of delivering customer location information with high precision, access to that system must be vigorously protected from outsiders. The best way to protect the system from misuse is to design it in such a way that it can only be triggered from the handset at the time a 911 call is placed, and that the handset only be allowed to respond to subsequent location data seeking pings from a wireless carrier within a reasonable period, such as 24 or 48 hours, after the call ends. Privacy advocates urged that the Commission require carriers to design with this important feature to protect consumers from being located for surveillance purposes, or by malicious hackers or foreign governments. Such a mechanism would build consent into the process of disclosing

[3] For example, Google allows consumers to opt out of having their devices included in the Google Location Service by appending "_nomap" to their SSID. *Configure Access Points with Google Location Service*, Google (last visited Jan. 22, 2015), https://support.google.com/maps/answer/1725632?hl=en.

sensitive, high-accuracy location data, and make sure that lives can be saved while not turning E911 into a surveillance tool that can be abused without the knowledge or consent of the handset owner.

Assurance that technologies designed to comply with E911 requirements (e.g., barometric sensors or firmware that determines location using WiFi and Bluetooth) will not be made available to third parties without consumers' express opt-in consent. Privacy advocates explained that this is a critical safeguard because consumers are highly protective of their location information. For example, last November the Pew Research Center reported that 82% of American adults consider 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."[4] Third parties should never have access to raw data or location information derived from technologies designed to comply with E911, except when consumers expressly opt in to sharing that information with third parties.

Assurance that, in accordance with their preferences, consumers will not only be able to turn location services on or off via a global setting on their mobile devices, but will also be able to granularly grant or deny access to location services to each application. Privacy advocates explained that consumers may wish to take advantage of new location technologies to share precise location information with some third-party applications, but not others, and should have the ability to make that determination on an application-by-application basis. For example, an aviation hobbyist may wish to allow access to the barometric sensor in his or her phone to a third-party app that displays and logs altitude data, but may not wish to allow the Facebook app to access to barometric sensor data. Some phones currently have granular settings that allow users to toggle location data on or off on an application-by-application basis, but others

[4] 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.

do not have such granular settings, instead only having one global option to have location services on or off. A consumer with a phone that only has a global setting for location services would not be able to grant access to location information to an aviation app while denying access to a Facebook app installed on the phone and running in the background. As mobile location data becomes more precise in accordance with updated E911 rules, consumers' interest in having granular settings for location services grows.

Assurance that information gathered from E911 technologies are not used by or disseminated to third parties, including government entities. The information gathered through E911 systems will be highly sensitive. Procedures should be put in place to ensure that such information is only used for E911 purposes, is purged within a limited proscribed timeframe, and is never sold or shared with third parties, including government entities.

Privacy advocates also asked that the Commission commit to putting out on public notice any privacy and security plans submitted by carriers for certification so that members of the public can review them and provide comments and feedback. The Commission should encourage carriers to consult with privacy and consumer organizations as they develop E911 technology and privacy and security plans. Consultation with all stakeholders throughout the process will increase the likelihood that privacy and security plans will be found satisfactory when they are ultimately put out on notice for public comment.

Privacy advocates asked that the Order include a clear commitment by the Commission to reviewing and updating its privacy rules in the near future. Privacy advocates explained that it would make sense for the Commission to review and update privacy rules in the context of the Technology Transitions docket.[5]

In addition, privacy advocates urged that the Commission consult with cybersecurity experts and require carriers to consult with cybersecurity experts as well as the E911 system is designed and deployed. The

[5] GN Docket No. 13-5.

Washington Post has published several articles in the past year exposing that major security flaws exist in the "SS7" networks used by wireless carriers in the United States.[6] These flaws can be used to locate individuals without their knowledge or consent, as well as without the knowledge or assistance of the wireless carriers. The existence of these security flaws, and the fact that private parties are already exploiting them for profit, demonstrates the critical need to consider cybersecurity as a basic requirement in any expansion of E-911.

Privacy advocates also explained that the Commission is well situated to address privacy concerns in the manner in which privacy advocates have outlined. The Commission provided all interested parties with notice that it was considering privacy issues in the Third Further Notice of Proposed Rulemaking in this docket.[7] The Commission also possesses ample authority to require carriers to build in specific privacy protections, and to update its privacy rules. Among the Commission's sources of authority in this area are the Commission's § 201(b) just and reasonable standard, § 222 authority governing CPNI, §§ 303(b) and (r) authority to set service rules, § 338 satellite privacy authority, and § 551 cable privacy authority. In addition, the Commission can regulate location information derived from technologies deployed by carriers to comply with the Commission's E911 as CPNI under the precedent set by the Commission's 2013 declaratory ruling regarding Carrier IQ, in which the Commission explained that "the 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

---

[6] Craig Timberg, *For Sale: Systems that Can Secretly Track Where Cellphone Users Go Around The Globe*, Washington Post (Aug. 8, 2014), *available at* http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html; Craig Timberg, *German Researchers Discover a Flaw that Could Let Anyone Listen to Your Cell Calls*, Washington Post (Dec. 18, 2014), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/.

[7] *Wireless E911 Location Accuracy Requirements*, Third Further Notice of Proposed Rulemaking (Feb. 20, 2014) at ¶ 136.

customers' devices when carriers or their designees have access to or control over that information."[8]

Although privacy advocates believe the Commission has ample authority to address privacy concerns in this docket, privacy advocates asked that the Commission not include language in the Order that would preserve the application of all valid severable parts of the Order in the event that one portion were found to be invalid. In the unlikely event that a portion of the Order addressing privacy concerns were to be struck down in court, it is critical that the Commission return to the drawing board for a solution, rather than letting precise location technology move forward without critical privacy and security safeguards.

Respectfully submitted,

/s/

Laura M. Moy
Open Technology Institute
New America
1899 L St, NW, Suite 400
Washington, DC 20036
(202) 596-3346

[8] *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.