



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:

On Wednesday, January 21, 2015, I spoke by phone with Louis Peraertz, Legal Advisor to Commissioner Clyburn regarding privacy concerns in the above-referenced docket. I expressed concerns regarding a recent filing posted to the docket by AT&T, Sprint, Verizon, and T-Mobile (collectively “carriers”). That filing states in relevant part:

Some concerns were also raised about the privacy and security of information contained in National Emergency Address Database (NEAD) used to validate reference points, including information specific to particular consumers or consumer-owned devices. As part of the ongoing effort to establish the NEAD, the signatory carriers have committed to engage with various industry experts on privacy and security to ensure that best practices are followed in the development and operation of the database. An additional commitment is made here to require the vendor(s) selected for the NEAD administration to develop a Privacy and Security Plan in advance of going live and transmit it to the FCC.

I told Mr. Peraertz that I believe the carriers’ recognition of privacy concerns is a step in the right direction, but that the measures outlined in carriers’ recent filing do not go nearly far enough toward addressing privacy

concerns that I and several other organizations have raised with the Commission.¹ As an initial matter, the carriers note that privacy- and security-related concerns have been raised about information contained in NEAD, but make no mention of the numerous other privacy concerns that I and others have raised regarding other aspects of the E911 system, in addition to concerns about NEAD.²

In addition, the carriers' offered solution—"to require the vendor(s) selected for NEAD administration to develop a Privacy and Security Plan"—raises additional concerns for the privacy community. While it is critical that any vendors file privacy and security plans, it is even more critical that the carriers themselves be required to file privacy and security plans, and that such plans address privacy and security with respect to the entire E911 system, not only with respect to NEAD. It is also extremely important that any privacy and security plans submitted to the FCC for certification be released on public notice before the FCC grants certification, to provide the public with an opportunity to review the plans and provide feedback.

I also emphasized to Mr. Peraertz that comprehensive privacy and security plans that will be put out on public notice down the road are necessary, but not sufficient to ensure that the updated E911 system incorporates privacy by design. That is why the Commission must tell carriers at this early point what it expects to see in privacy and security plans to be filed in the future.

I told Mr. Peraertz that the carriers must also consult with privacy organizations. The carriers "have committed to engage with various industry experts on privacy and security to ensure that best practices are followed in the development and operation of the database." But to ensure that the E911 system and the technologies that will be deployed to comply with E911 rules are designed responsibly from the ground up with respect to privacy and security, the carriers must commit to engaging with more than merely "industry experts on privacy and security." The carriers must include a

¹ 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>.

² *Id.*

number of stakeholders from the privacy, security, and consumer communities in the design and deployment of E911.

To address privacy concerns, carriers and the Commission should look to the letter filed in this docket on January 13th by New America's Open Technology Institute, American Civil Liberties Union, American Library Association, Benton Foundation, Brennan Center for Justice, Center for Democracy & Technology, Center for Digital Democracy, Consumer Action, Consumer Federation of America, Consumer Federation of California, Consumer Watchdog, Defending Dissent Foundation, Electronic Frontier Foundation, Public Knowledge, Privacy Rights Clearinghouse, Sunlight Foundation, U.S. PIRG, and World Privacy Forum.³ In that letter, privacy advocates argued that carriers should be required to commit to the following:

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”). 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.

A system design in which E911 location functionality can only be triggered through the handset, and not remotely. 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, such as malicious hackers and foreign governments. 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.

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

³ 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>.

opt-in consent. 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

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. 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.

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.

Respectfully submitted,

/s/

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

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.