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 AND
ELECTRONIC PRIVACY INFORMATION CENTER

I. INTRODUCTION

Public Knowledge (PK) and Electronic Privacy Information Center (EPIC) submit these Comments in response to the Commission's Sixth Further Notice of Proposed Rulemaking in this docket seeking public comment on improvements to wireless E911 location accuracy rules.[1] PK and EPIC believe that a robust wireless 911 (or E911) service that collects precise and accurate location data is important to help the public to quickly receive emergency services in moments where help is needed the most. However, as the collection of sensitive information increases, the need to protect such data rises too. The Commission has presented acceptable proposals to make E911 better, but has failed to properly consider in its proposals the importance of consumer privacy. The Commission, before adopting any new E911 rules, should therefore seek further comment on how to protect subscriber information, including Customer Proprietary Network Information (CPNI),[2] as demands for sensitive location data increase. A proper balance must be struck between the benefits of using more actionable location data and keeping such data secure in order to ensure that public safety goals do not compromise consumer protections.

[1] *Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Sixth Further Notice of Proposed Rulemaking, FCC 25-22 (Mar. 28, 2025) ("*Sixth NPRM*").
[2] 47 U.S.C. § 222.

II. ROBUST PRIVACY PROTECTIONS ARE IMPORTANT TO PROTECT CONSUMERS IN CRITICAL TIMES OF NEED

As outgoing Commissioner Starks said, "[w]hile precise location information is critical to an effective emergency response, it can also be dangerous in the wrong hands."[3] The next generation of E911 entails enhanced 911 services that include precise location information that can be used to enable Public Safety Answering Points (PSAPs) and first responders to better serve the public. However, there are grave concerns over the handling of sensitive location data by carriers. As Commenters have consistently advocated since the opening of this docket, enhancing 911 is commendable but only as long as the Commission complies with its obligation to protect the privacy of consumer information generated by the provision of communication services.[4]

The CNPI rules provide standards that must pave the way for how the Commission frames protecting consumers in light of enhancements to 911 services. These rules, which protect consumers from pervasive collection of personal data including the type of service a customer uses, a customer's usage details (e.g., call logs, call duration, call destinations), billing records, and location data, should apply to all calls made to PSAPs and emergency services and to the data collected from such calls. While consent is not necessary for calls to 911,[5] carriers and 911 providers who take and process E911 location data are subject to privacy rules, which include CPNI reporting and certifications, breach reporting, and other standards that protect sensitive

[3] *See, e.g.*, *Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Statement of Commissioner Geoffrey Starks, FCC 20-98 (July 17, 2020).
[4] *See e.g.*, Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114, Comments of Public Knowledge (May 20, 2019); Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114, Comments of Public Knowledge et al. (Dec. 14, 2014); Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114, Comments of Electronic Privacy Information Center (Aug.10, 2007); *Location-Based Routing for Wireless 911 Calls*, PS Docket No. 18-64, Comments of Electronic Privacy Information Center (Feb. 16, 2023).
[5] 47 U.S.C. § 222(d)(4) (limiting exceptions for disclosure of CPNI).

consumer data.[6] These rules as applied to E911 must protect subscriber data on a two-fold basis, preventing that data from being disclosed or misused by unauthorized users[7] and to prevent data from being misused by the companies themselves.[8] As more sensitive data is collected, more safeguards must be required to balance public safety goals with consumer protection.

III. COMMENTERS SUPPORT THE COMMISSION'S BROAD GOALS RELATED TO IMPROVING LOCATION ACCURACY IN E911, PROVIDED ADEQUATE PRIVACY PROTECTIONS ARE IN PLACE

The Commission's goal to make E911 data more reliable and actionable for providing faster emergency responses is commendable. Improvements to z–axis data will make 911 services better, and Commenters support the Commission's initiatives here. Currently, as providers deliver the z-axis component in Height Above Ellipsoid (HAE) to PSAPs, as the Commission well knows, location data accuracy is limited and imprecise. The proposal to switch to providers providing both the HAE and Above Ground Level (AGL) values with each call can increase the reliability and actionability of z-axis data but also will double the amount of

[6] 47 U.S.C. § 222(d)(4)(A). PSAPs are not themselves carriers, but carriers have the obligation to ensure that the disclosure to PSAPs does not allow third parties to use the information in a way not permitted by Section 222(d)(4).

[7] *See e.g*., *Data Breach Reporting Requirements,* WC Docket No. 22-21, Comments of Electronic Privacy Information Center, et al. (Mar 24, 2023) (providing examples of the harm of employee data breaches resulting in data being sold); *Nation's Communications Systems from Cybersecurity Threats*, PS Docket NO. 22-329, Electronic Privacy Information Center's Opposition to Petition for Reconsideration (Mar. 3, 2025) (petitioning to require carriers to implement basic cybersecurity safeguards in the wake of "the most significant and far-reaching cyber [incident] in U.S. history.").

[8] Evidence demonstrates that mobile carriers themselves have violated CPNI rules and even try to avoid § 222 requirements. *See e.g.*, Brief of Electronic Privacy Information Center, Center for Democracy & Technology, Electronic Frontier Foundation, Privacy Rights Clearinghouse, and Public Knowledge as Amici Curiae in Support of the FCC's Forfeiture Order, *In re Verizon Communications*, File No. EB-TCD-18- 00027698, FCC 24-41 (Jan. 24, 2025); Brief of Electronic Privacy Information Center, Center for Democracy & Technology, Electronic Frontier Foundation, Privacy Rights Clearinghouse, and Public Knowledge as Amici Curiae in Support of the FCC's Forfeiture Order, *In re Sprint Corp.*, File No. EB-TCD-18-00027700, FCC 24-42; and *In re T-Mobile USA, Inc.*, File No. EB-TCD-18-00027702, FCC 24-43 (Jan. 17, 2025).

sensitive z-axis data collected, thereby increasing the need for greater privacy protections. The Commission should take this into account when considering how to ensure that subscriber data is protected. Next, requiring that providers deliver floor level estimates will be helpful to first responders and boost public safety, but just as with AGL values, these estimates necessarily increase that amount of data that PSAPs collect and therefore inherently increase the importance of protecting CPNI and other subscriber data in the E911 ecosystem. Finally, Commenters support the Commission's goals of generally strengthening the wireless 911 location accuracy testing and compliance framework, as strengthening testing requirements and improving the provision of dispatchable locations to PSAPs will help E911 to be more robust and enable first responders to provide better emergency services to consumers. Overall, however, the public interest benefits of these proposals will be diminished if the Commission does not prioritize protecting subscriber privacy.

IV. THE COMMISSION MUST CONSIDER AND DEVELOP THE RECORD FURTHER AS RELATED TO CONSUMER PRIVACY CONCERNS FOR SENSITIVE E911 LOCATION DATA

As Commenters have demonstrated, the safety of sensitive subscriber data associated with E911 services is critical to ensuring that consumer interests are not compromised for enhancements in public safety. Indeed, this is a false choice. The Commission easily can (and must) take an approach that boosts both privacy protections and overall public safety. The following are some specific considerations that should be made in regard to the proposals in the Sixth Further Notice of Proposed Rulemaking.

Third Parties and CNPI Protection. When allowing third party services to access CPNI and other subscriber data related to E911 services, whether for accessing test data to make location data more usable or for conveying dispatchable locations, it is critically important to

ensure that these third parties comply with the Commission's subscriber privacy rules.[9] The Commission should adopt rules that explicitly require all third parties interacting with dispatchable location data to comply with its standards for subscriber privacy.

Testing and Compliance Framework. As the wireless 911 location accuracy testing and compliance framework is updated or enhanced, the Commission must ensure that all testing data is analyzed and treated accordingly with standards such as the National Emergency Address Database (NEAD) and CPNI rules.[10] Furthermore, the Commission should consider the importance of removing all personalized information from testing data to increase anonymity for data used outside of emergency responses.

Use of New Technologies for Dispatchable Locations. Historically, PSAPs have been provided dispatchable location information from service providers using cellular networks and more recently GPS information from mobile devices. In exploring the use of new technologies for location reporting, such as 5G networks, Wi-Fi networks, and the Internet of Things (IoT), the Commission should seek further comment related to the privacy implications of using such technologies.[11] These networks are increasingly sensitive and can not only expose consumers' information but can also relay information about relationships among devices and networks that are not necessarily required for accurate reportable locations.

Privacy Framework for Data. If the Commission were to develop a new database for E911 locations, or use a private database, it must ensure that consumer data is protected in accordance with relevant subscriber privacy standards.[12] And as the Commission considers

[9] *Sixth NPRM* at ¶¶ 35, 53.
[10] *Sixth NPRM* at ¶¶ 26-38.
[11] *Sixth NPRM* at ¶¶ 44-52.
[12] *Sixth NPRM* at ¶¶ 35, 56-7.

reporting requirements related to databases, the Commission must ensure that all data portals are secure and anonymized. Furthermore, the Commission should remind all CMRS providers the continuing obligations they have regarding privacy without the NEAD and also carry over NEAD accountability provisions if NEAD provisions are being considered for deletion. All information associated with dispatchable location information, whether stored in the NEAD or not, must receive the highest degree of protection. This should include maintaining an appropriate standard of security to prevent unintended disclosures over and above the requirements already imposed by the Commission to protect CPNI.

The Commission has adopted "broad privacy protections" that "apply to any data that is shared" that require all Commercial Mobile Radio Service (CMRS) providers to "safeguard the privacy and security of emergency location data throughout all elements of their systems for determining 911 location and delivering location information to PSAPs" and similarly apply to third party vendors.[13] The NEAD protections stretch past NEAD data only, applying also to non-NEAD dispatchable location data that is stored and additionally create privacy protection obligations for dispatchable location data that apply to location information used for location-based routing, including device-based location data.[14] If the Commission were to eliminate any NEAD rules, it should remind providers that these mirrored obligations for non-NEAD dispatchable location data would persist.

---

[13] *Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Sixth Report and Order and Order on Reconsideration, 35 FCC Rcd 7752 (2020) at ¶ 57, corrected by Erratum (PSHSB Aug. 28, 2020) and Second Erratum (PSHSB Oct. 29, 2020) ("*Sixth R&O*"); *see also Location-Based Routing for Wireless 911 Calls*, PS Docket Nos. 21-479 and 18-64, Report and Order, FCC 24-78, 2024 WL 3507091 at ¶ 102 (July 19, 2024), corrected by Erratum, 2024 WL 3507091 (Sept. 5, 2024) and Second Erratum, 2024 WL 3507091 (Oct. 1, 2024).

[14] *Id.* at ¶ 103; *Sixth R&O* at ¶ 56.

In moving on from NEAD, the Commission should also consider importing NEAD requirements generally to any database used to collect dispatchable location data. Non-NEAD rules only require certifications in correspondence with CPNI rules, but NEAD requires a documented plan with a designated point of accountability, heightened protections for stored data, and greater protections against invalid government requests for data.[15] The NEAD framework can be extended to apply to all sensitive location data, including not only data that is stored in a database but also data that is deleted or being transferred. The Commission should inquire further about such privacy rules and consider establishing a blanket framework for protecting sensitive E911 data at all times for CMRS providers, PSAPs, emergency responders, third parties, and more.

Deletion of Rules. The Commission should not delete any rules related to the protection of CPNI (or consumer protection in general) in this rulemaking, especially without proposing a suitable replacement for such rules.[16] Importantly, the Commission must not delete the NEAD definition in section 9.10(i)(1)(iii) and requirements to submit a privacy and security plan for the NEAD under section 9.10(i)(4)(iii) without supplementing similar privacy rules.[17] If any rules are deleted, newly proposed rules must contemplate the protection of consumer privacy.

V. CONCLUSION

For the reasons stated above, the Commission should ensure and reaffirm that any CPNI included in data from CMRS providers transferred to, stored by, or even deleted by PSAPs, first responders, or third parties is protected to the largest extent possible.

---

[15] *See* 47 CFR 9.10(i)(4). "The plan must include the identity of an administrator for the NEAD, who will serve as a point of contact for the Commission and shall be accountable for the effectiveness of the security, privacy, and resiliency measures."
[16] *Sixth NPRM* at ¶¶ 69-79.
[17] *Sixth NPRM* at ¶ 77.

Respectfully submitted,

/s/ Peter Gregory
/s/ Harold Feld
Public Knowledge
1818 N Street NW, Suite 410
Washington, DC 20036

/s/ Chris Frascella
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036

June 6, 2025