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

In the Matter of	)	
	)	
Facilitating Implementation of Next Generation 911 Services (NG911)	)	PS Docket No. 21-479
	)	
	)	
Improving 911 Reliability	)	PS Docket No. 13-75

COMMENTS OF PUBLIC KNOWLEDGE

I. INTRODUCTION

Public Knowledge (PK) submits these Comments in response to the Commission's Further Notice of Proposed Rulemaking seeking to update its rules to improve the resiliency, reliability, interoperability, and accessibility of Next Generation 911 (NG911) networks.[1] PK strongly supports the Commission's initiatives to enhance 911 networks and specifically supports the Commission's goals in this proceeding to make NG911 more reliable and useful for consumers who require emergency services in critical times of need. However, these services do not come without risks. PK, as it has long supported, urges the Commission to prioritize the protection of consumer information and related sensitive data that is transmitted through the use of NG911 services as it considers enhancing NG911 networks. As the use of these NG911 services–which are a vital lifeline for consumers during times of necessity–increases, the risks of the misuse and exposure of sensitive consumer information grow in tandem.

[1] *Facilitating Implementation of Next Generation 911 Services (NG911)*, Further Notice of Proposed Rulemaking, PS Docket Nos. 21-479, 13-75 (Mar. 28, 2025) ("*NG911 FNPRM*").

While the Commission has proposed acceptable solutions to help make NG911 better, it has failed to properly consider the importance of protecting sensitive consumer information – just as in the concurrent E911 proceeding.[2] Therefore, before adopting any new NG911 rules, the Commission should seek further comment on how to protect subscriber information, including Customer Proprietary Network Information (CPNI),[3] as the use of sensitive consumer data for NG911 services increases. A proper balance must be struck between the benefits of using more data for NG911 services and keeping such data secure in order to ensure that public safety goals do not compromise consumer protections.

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

As PK has advocated, enhancing 911 services is commendable but only as long as the Commission complies with its statutory obligation to protect the privacy of consumer information generated by the provision of communication services.[4] The CPNI rules provide standards that must pave the way for how the Commission frames protecting consumers in light of enhancements to all next-generation 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, location data, and more should apply to all calls, texts, and transmissions otherwise made to PSAPs and emergency services and the data that is then collected from such interactions. While consent is not necessary

[2] *Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Sixth Further Notice of Proposed Rulemaking, FCC 25-22 (Mar. 28, 2025).
[3] 47 U.S.C. § 222.
[4] *See e.g.*, Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114, Comments of Public Knowledge and EPIC (Jun. 6, 2025); 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).

for calls to 911,[5] carriers and 911 providers who take and process NG911 call, text, and/or location data are subject to privacy rules, which include CPNI reporting and certifications, breach reporting, and other standards that protect sensitive consumer data.[6] These rules, as applied in the NG911 context, must protect subscriber data on a two-fold basis, preventing data from being disclosed or misused by unauthorized users[7] and preventing data from being misused by the companies themselves.[8] In line with the Communications Security, Reliability, and Interoperability Council (CSRIC) recommendation in the CSRIC VII Report *Measuring Risk Magnitude and Remediation Cost in 911 and NG911 Networks*, cybersecurity and, in turn, the protection of sensitive CPNI, should be priorities for the Commission during the NG911 transition.[9] Therefore, as more sensitive data is collected and threats increase, more safeguards must be required to balance public safety goals with consumer protection.

---

[5] 47 U.S.C. § 222(d)(4) (limiting exceptions for disclosure of CPNI).
[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).
[9] CSRIC VII, Report on the Current State of Interoperability in the Nation's 911 Systems (Mar. 10, 2021), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-Interoperability-council-vii.

III. PUBLIC KNOWLEDGE SUPPORTS UPDATING THE COMMISSION'S RULES TO PROMOTE RELIABILITY, INTEROPERABILITY, AND ACCESSIBILITY OF NG911 NETWORKS.

In general, PK supports the Commission's initiative to "update existing Commission rules to ensure the resiliency, reliability, interoperability, and accessibility" for NG911, given the Commission's public interest duty to ensure that 911 networks are resilient and reliable.[10] As such, PK believes that the proposed measures in the *NG911 FNPRM* will improve NG911 networks to better serve the public interest.

A. THE COMMISSION SHOULD EXPAND THE DEFINITION OF A "COVERED 911 SERVICE PROVIDER" TO HOLD NG911 ENTITIES TO SIMILAR RELIABILITY REQUIREMENTS AS LEGACY 911 SYSTEMS.

Public Knowledge broadly supports the Commission's objective of expanding the definition of a Covered 911 Service Provider (CSP) to include the services that are used throughout the entire NG911 ecosystem. Doing such will enable the Commission to ensure the multiple components that make up the NG911 system are reliable and, further, to ensure that the newly-expanded list of CSPs handles CPNI appropriately. In specific, PK supports expanding the definition of "CSP" past just the systems that serve the functional equivalent of legacy 911 service providers to include, as proposed, "(1) operators of Location Information Servers (LISs) or equivalent IP 911 location databases; (2) operators of Legacy Network Gateways (LNGs); (3) operators of interstate Major Transport Facilities that meet or exceed Optical Carrier 3 (OC3) capacity and carry 911 traffic from multiple OSPs for ultimate delivery to NG911 Delivery Points or ESInets; (4) operators of IP Traffic Aggregation Facilities that carry segregated 911 traffic from multiple OSPs towards ultimate transmission to an NG911 Delivery Point or ESInet; and (5) operators of interstate interconnecting facilities between ESInets."

[10] 47 U.S.C. §§ 151, 615.

As the Commission expands this definition, it must ensure that all services that handle consumer data in critical times, whether at the genesis of a call, after a PSAP has received information, or even after a call is completed, are included and regulated as CSPs. Anything "critical to the overall reliability of the 911 ecosystem" should be considered a CSP in order to ensure that each part of the NG911 network, as well as the 911 network as a whole, is reliable and held to standards that put the consumer first.

B. ENHANCING RELIABILITY AND RELATED CERTIFICATION REQUIREMENTS WILL MAKE 911 NETWORKS MORE RESILIENT AND SERVE THE PUBLIC INTEREST.

Public Knowledge supports keeping the "reasonableness standard" in section 9.19 of the Commission's rules requiring CSPs to take "reasonable measures" to ensure reliability, as this is a robust requirement that supports the broader public interest. Additionally, PK supports including additional "best practice" benchmarks for CSPs to meet for further certification purposes. However, these benchmarks as proposed may fall short in addressing consumer privacy and other consumer safety risks. As such, the Commission should require at a minimum that CSPs comply duly with consumer data privacy and other CPNI requirements as additional "best practice" benchmarks.

C. INTEROPERABILITY WILL ALLOW NG911 NETWORKS TO SERVE CONSUMERS BETTER, REDUCE POINTS OF FAILURE, AND MAKE NG911 SERVICES MORE ACCESSIBLE.

Public Knowledge supports interstate interoperability requirements that will enhance the reliable exchange of interstate 911 traffic between ESInets. Interoperability is important to ensure that NG911 networks work well, especially throughout the transitional period between legacy 911 and NG911 services. This includes interoperability for text and video, as this will make 911 services more accessible universally. A requirement for CSPs to certify interoperability, as the Commission has proposed, will help to ensure that NG911 networks work

with legacy technology. Requiring interoperability will also help the Commission ensure a continued smooth path to facilitate the NG911 transition.

IV. THE COMMISSION SHOULD IMPROVE NG911 NETWORKS BY PROMOTING CONSUMER PRIVACY AND TRANSPARENCY.

Despite the proposed improvements to NG911 in the *NG911 FNPRM*, the Commission fails to consider the vast public interest implications that the NG911 system has on the security and safety of sensitive consumer information, or CPNI, that is transmitted during the NG911 lifecycle. While PK generally supports the Commission's initiatives to enhance oversight into the reliability certification process based on "reasonableness" and make this process more transparent, the *NG911 FNPRM* falls short because it does not ensure that sensitive CPNI is secured and treated properly to prevent illicit disclosure. Such threats risking the unauthorized exposure of CPNI, from cybersecurity breaches or even the companies within the NG911 ecosystem itself, are not new. In 2020, the Commission proposed an over $200 million fine to major wireless carriers for selling access to customers' real-time location data.[11] And, in 2022, Intrado experienced a cyberattack on its 911 infrastructure, risking the release of sensitive CPNI if ransom demands were not met.[12] As the data used in NG911 is richer and more robust, the risk–threat even–of unauthorized or illegal exposure of CPNI is likely to grow. The Commission must do more to ensure that the protection of CPNI is prioritized alongside its public safety goals.

---

[11] *See e.g., Sprint Corporation,* Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1655 (2020); *T-Mobile USA, Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1785 (2020).

[12] Vlad Constantinescu, *Royal Ransomware Group Claims Attack Against Intrado Telecom Company* (Dec. 29, 2022), available at https://www.bitdefender.com/en-us/blog/hotforsecurity/royal-ransomware-group-claims-attack-against-intrado-telecom-company.

A. THE COMMISSION SHOULD ESTABLISH ADDITIONAL REQUIREMENTS FOR CSPS TO CERTIFY THAT THEY COMPLY WITH ACCEPTED CONSUMER PRIVACY STANDARDS.

As the Commission seeks to update the requirements for NG911, it must consider the relevant privacy safety standards it is subject to. These CPNI Standards, in Section 222 of the Communications Act, prescribe an affirmative duty for telecommunications carriers to "protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers…"[13] While CPNI can be transmitted by carriers to PSAPs and other services within the 911 ecosystem for the provision of emergency services, this does not mean that the Commission's duty to protect from the misuse or otherwise unauthorized disclosure of CPNI is lost or less important. To safeguard against unauthorized disclosure risk, the Commission should require CPNI compliance and certifications within the NG911 framework it has proposed, and further ensure that the certifications are renewed yearly. This certification should also develop a mechanism that allows the Commission regular oversight into whether providers are actually following the certification standards with regard to the protection of CPNI and properly complying with reporting requirements when CPNI is improperly disclosed or mismanaged. Such certification and associated requirements can help to ensure that CPNI is properly handled in each component of the NG911 network.

B. THE COMMISSION SHOULD SEEK FURTHER COMMENT ON HOW CSPS DELIVER, USE, AND STORE SENSITIVE NG911 INFORMATION.

The Commission has already 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

[13] 47 U.S.C. § 222.

similarly apply to third party vendors.[14] As such, the Commission should seek more information on how data is used, stored, accessed, transmitted, and otherwise used throughout the NG911 network ecosystem to determine the particular CPNI-exposure risks, what processes CSPs have in place to mitigate risks, and how the Commission's oversight can be used to ensure that CPNI is protected as required by law. The Commission should also direct the Communications Security, Reliability, and Interoperability Council (CSRIC) to conduct a comprehensive study and report on safeguarding CPNI in NG911 networks.

C. THE COMMISSION SHOULD ESTABLISH A MECHANISM FOR CONSUMER COMPLAINTS RELATED TO NG911 OUTAGES FOR ENHANCED TRANSPARENCY.

Finally, the Commission should establish a mechanism, such as a consumer web portal, to increase transparency in NG911 and enhance communication between the FCC and consumers on the provision and availability of NG911 services. This mechanism should allow consumers to file complaints related to the NG911 network or system outages in order to help the Commission identify any CSP that is not reliably performing in accordance with its certification requirements and then easily investigate whether CSPs are in compliance with their duty to take "reasonable measures" to ensure reliability. Such a mechanism that allows for real-time reporting of NG911 outages is critical to ensuring that everyone has access to reliable NG911 services.

V. CONCLUSION

For the reasons stated above, the Commission should update its rules to improve the resiliency, reliability, interoperability, and accessibility of NG911 networks, and also take further

[14] *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).

steps to ensure and reaffirm that any CPNI included in data transferred to, stored by, or even deleted by CSPs in the provision of NG911 services is protected to the largest extent possible.

Respectfully submitted,

/s/ Peter Gregory
Broadband Policy Fellow
Public Knowledge
1818 N Street NW, Suite 410
Washington, DC 20036

August 4, 2025