Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Nation's Communications	)	PS Docket No. 22-329
Systems from Cybersecurity Threats	)	

OPPOSITION TO PETITION FOR RECONSIDERATION OF CTIA – THE WIRELESS ASSOCIATION, NCTA – THE INTERNET & TELEVISION ASSOCIATION, AND USTELECOM – THE BROADBAND ASSOCIATION

The Electronic Privacy Information Center (EPIC) respectfully submits this Opposition to the Petition filed by carrier associations CTIA, NCTA, and USTelecom for Reconsideration[1] of the Federal Communications Commission's ("FCC" or "Commission") Declaratory Ruling ("Ruling")[2] requiring carriers to implement basic cybersecurity safeguards in the wake of what has been characterized as "the most significant and far-reaching cyber [incident] in U.S. history."[3] The breach—which was revealed to the public in October and is still ongoing in February[4]—was so severe that the Federal Bureau of Investigation has urged Americans to rely on end to end encrypted messaging instead of text messaging.[5]

[1] Petition for Reconsideration of CTIA, NCTA, USTelecom, *In re Protecting the Nation's Communications Systems from Cybersecurity Threats,* PS Dkt. No. 22-329 (Feb. 18, 2025), https://www.fcc.gov/ecfs/document/102183024015116/1 ("PFR").
[2] Declaratory Ruling and Notice of Proposed Rulemaking, PS Dkt. No. 22-329 (Rel. Jan. 16, 2025), https://docs.fcc.gov/public/attachments/FCC-25-9A1.pdf ("Ruling").
[3] Federal Communications Commission, December 2024 Open Commission Meeting at 50:18 (Dec. 11, 2024), https://www.youtube.com/watch?v=1sTo_oZSQ9Q&t=3018s (comment of Comm'r Carr at press conference following Comm'n meeting).
[4] *See* Matt Kapko, *Salt Typhoon remains active, hits more telecom networks via Cisco routers*, CyberScoop (Feb. 13, 2025), https://cyberscoop.com/salt-typhoon-china-ongoing-telecom-attack-spree/.
[5] *See* Zak Doffman, *FBI Warns iPhone and Android Users—Stop Sending Texts*, Forbes (Dec. 6, 2024), https://www.forbes.com/sites/zakdoffman/2024/12/06/fbi-warns-iphone-and-android-users-stop-sending-texts/.

The deficient cybersecurity of America's communications networks sadly is well-documented at this point[6]—although the full scope of the risks and harms both incurred and ongoing remains hidden from the public.[7] In a cynical turn, it is the same carriers on whose watch this egregious, unprecedented breach was permitted to occur who now bemoan and frustrate the FCC's efforts to remedy the situation. They seem to argue that Congress somehow intended for the Communications Assistance for Law Enforcement Act (CALEA) to create a sort of safe harbor for insecure cybersecurity practices, and that the agency with the clearest responsibility over common carriers and over our nation's communications infrastructure has exceeded its authority by requiring carriers to do better by the American people.

EPIC was founded in the same year as Congress enacted CALEA,[8] and since its inception EPIC has advocated for greater oversight and accountability of these uniquely dangerous law enforcement surveillance systems that put private communications at risk.[9] CALEA requires carriers to ensure continued government interception capabilities as communications technology changes, balancing three key policies:

---

[6] *See, e.g.*, EPIC Testifies at House Hearing on Securing Communications Networks (Jan. 10, 2024), https://epic.org/epic-testifies-at-house-hearing-on-securing-communications-networks/; Reply Comment of EPIC, *In re Public Safety and Homeland Security Bureau Requests Comment on Implementation of Measures to Prevent Location Tracking via the Diameter and Signaling System 7 Security Protocols*, PS Dkt. No. 18-99 (May 28, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1052800568030.

[7] *See, e.g.*, Lorenzo Franceschi-Bicchierai, *Trump administration fires members of cybersecurity review board in 'horribly shortsighted' decision*, TechCrunch (Jan. 22, 2025), https://techcrunch.com/2025/01/22/trump-administration-fires-members-of-cybersecurity-review-board-in-horribly-shortsighted-decision/; EPIC Seeks CISA Report on Threat of SS7 Surveillance (Mar. 13, 2024), https://epic.org/epic-seeks-cisa-report-on-threat-of-ss7-surveillance/. *See also* Letter from Ron Wyden, U.S. Sen., to Hon. Jen Easterly, Dir. Cybersecurity and Infrastructure Security Agency, and Hon. Paul M. Nakasone, Dir. National Security Agency (Apr. 12, 2023), https://www.wyden.senate.gov/imo/media/doc/FirstNet%20security%20letter%20to%20CISA%20and%20NSA%20FINAL.pdf.

[8] *See, e.g.*, H.R.4922 – Communications Assistance for Law Enforcement Act, https://www.congress.gov/bill/103rd-congress/house-bill/4922; About Us, EPIC, https://epic.org/about/ (last visited Feb. 28, 2025).

[9] *See, e.g.*, EPIC on Wiretap Bill Passage, *available at* https://archive.epic.org/privacy/wiretap/calea/epic_calea_statement.html (last visited Feb. 28, 2025); Wiretapping, EPIC, https://epic.org/issues/surveillance-oversight/wiretapping/ (last visited Feb. 28, 2025).

> (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.[10]

Petitioners' actions have failed to protect the privacy of Americans' data and failed to safeguard the security of our country's communications networks. And now Petitioners rebuke the FCC's Declaratory Ruling and offer instead the demonstrably inadequate status quo of self-regulation.

For decades, cybersecurity experts and privacy advocates have warned about the precise risk that was exploited in the Salt Typhoon incident—that the creation of backdoor access for the government would create an opening for malicious hackers.[11] And now millions of communications are at risk because of a security loophole in the law enforcement access system; there is no such thing as a backdoor that only good guys can use.

Petitioners claim the FCC's Ruling attempts to create a general cybersecurity regulation,[12] and that CALEA does not allow for this[13]—they are mistaken on both counts. The Commission's Ruling does not establish general cybersecurity regulations, it merely lays out precautions that must be in place to ensure that a carrier's compliance with CALEA does not come at the unacceptable expense of exacerbating existing nor creating new vulnerabilities.[14] And as the FCC compellingly noted in its Ruling: Congress explicitly changed the language of

---

[10] H.R. Rep. No. 103-827, 103d Cong., 2d Sess., pt. 1, at 13 (1994).
[11] *See, e.g.*, Susan Landau, *CALEA was a National Security Disaster Waiting to Happen*, Lawfare (Nov. 13, 2024), https://www.lawfaremedia.org/article/calea-was-a-national-security-disaster-waiting-to-happen; Communications Assistance for Law Enforcement Act (CALEA), Electronic Frontier Foundation, https://w2.eff.org/Privacy/Surveillance/CALEA/ (last visited Feb. 28, 2025); Cory Doctorow, *China hacked Verizon, AT&T, and Lumen using the FBI's backdoor*, Medium (Oct. 7, 2024), https://doctorow.medium.com/https-pluralistic-net-2024-10-07-foreseeable-outcomes-calea-4e543eb51bad; Zack Whittaker, *The 30-year-old internet backdoor law that came back to bite*, TechCrunch (Oct. 7, 2024), https://techcrunch.com/2024/10/07/the-30-year-old-internet-backdoor-law-that-came-back-to-bite/.
[12] *See* PFR at 4-5, 8.
[13] *See id.* at 8-11.
[14] As a practical matter, making compliance with CALEA conditional upon maintaining adequate cybersecurity measures may result in the majority of voice service providers having to adopt these measures, but that does not transmute statutorily-granted authority into an *ex nihilo* regulatory overreach.

the authorizing legislation to "any interception" rather than the narrower "any court ordered or lawfully authorized interception."[15] There is no room to interpret the intention of Congress otherwise.

But Petitioners go even further, arguing that: "Congress enacted CALEA to impose a narrow obligation on providers to facilitate lawful intercepts from law enforcement—regardless of what technical standards providers used to secure their networks",[16] and that deficient standards have not been alleged here[17]—they are again wrong on both the law and the facts. As noted above, a key priority of CALEA is to protect the privacy of communications—technical standards that do not meet this requirement have failed to comply with CALEA. Congress did not enact CALEA as a means for carriers to justify negligent cybersecurity by arguing that they are free from scrutiny so long as they are providing lawful access to sensitive communications data. And as a factual matter, the Ruling outlined the necessity for the Commission's timely action: namely, the manifest deficiency of carriers' current standards.[18]

The FCC's Ruling was a stopgap measure, urgent and responsive to our nation's current communications cybersecurity crisis. It is irresponsible of carriers to attempt to discard this measure without first implementing a better plan, and it is evident that the status quo is not equal to that task. The Commission should act swiftly to halt CALEA functionality until these vulnerabilities are resolved, to deftly solve an urgent problem rather than do nothing in the face of one of the most significant and far-reaching cyber incidents in U.S. history.

Respectfully submitted,

Alan Butler
/s/ Alan Butler
Executive Director

Chris Frascella
/s/ Chris Frascella
Counsel

Electronic Privacy Information Center (EPIC)
1519 New Hampshire Ave NW
Washington DC 20036

February 28, 2025

[15] *See* Ruling at ¶ 13.
[16] PFR at 4-5.
[17] *See* PFR at 8-9.
[18] *See, e.g.*, Ruling at ¶¶ 2-4.