epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Review of International Section 214	)	IB Docket No. 23-119
Authorizations to Assess Evolving National	)	
Security, Law Enforcement, Foreign Policy,	)	
and Trade Policy Risks	)	

REPLY COMMENTS ON NOTICE OF PROPOSED RULEMAKING

by

Electronic Privacy Information Center (EPIC)

Submitted October 2, 2023

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Summary

We applaud the Federal Communications Commission ("FCC" or "Commission") for its continued attention to data security concerns in this rulemaking. Data privacy and data security are of great concern to American consumers. In the absence of comprehensive federal legislation, a regulatory approach is a necessary stopgap to safeguard consumer interests and restore trust in our communications infrastructure.

We support the Commission's proposals to require certification of compliance with baseline cybersecurity requirements and to require re-certification, but with the caveats that auditing must be independent and thorough and that the Commission must bring enforcement actions against false certifications. Additionally, the extent of an audit should be risk-based and not solely size-based, and re-certification should occur annually. We also take the opportunity to address several challenges to the Commission's authority raised by commenters.

We strongly support the Commission's attempts to elevate the trajectory of telecom data security and urge the Commission to maintain consumer safety as the core goal of this proceeding.

Table of Contents

Summary **ii**

I. Introduction **1**

II. Cybersecurity and Data Privacy Threats Demand Commission Action. **2**

III. The Commission Should Enforce Adequately Independent, Thorough Audits that Align with Meaningful Cybersecurity Frameworks. **7**

IV. Audits Should Be Risk-Based in Scope, and Certifications Should Occur Annually. **12**

V. Challenges to the Commission's Proposals Raised by Commenters Do Not Preclude Commission Action. **13**

a. The Commission's Proposals Fall Within the Scope of its Authority Under Sections 201(b) and 4(i). 13

b. Challenges Based Upon the Major Questions Doctrine and the Congressional Review Act Necessarily Fail. 16

c. Risk-Based Auditing Mitigates Over-inclusivity, Articulating the Scope of Immediate Commission Priorities Mitigates Under-inclusivity. 18

VI. Conclusion **19**

Comments

I. Introduction

The Federal Communications Commission ("Commission" or "FCC") requested comment on its Notice of Proposed Rulemaking (NPRM) addressing the cybersecurity of telecommunications networks through its oversight of international authorization holders.[1] The **Electronic Privacy Information Center (EPIC)** files these reply comments to applaud the Commission for its attention to data security concerns and to support the agency's proposals—but with important caveats. We urge the Commission to require annual cybersecurity audits conducted by independent and thorough auditors. The scope of these audits should be risk-based, and the audits should inform annual certifications to the Commission. We support the Commission's use of its 201(b) and 4(i) authority to implement this regulation to maintain consumer trust in our communications networks, and we respond to several challenges to the Commission's authority raised by commenters.

EPIC[2] is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC has long defended the rights of consumers and has played a leading role in developing the Commission's authority to address emerging privacy and cybersecurity issues.[3] EPIC routinely advocates before the Commission for rules that protect consumers from exploitative or

[1] *In re* Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, Order and Notice of Proposed Rulemaking, IB Docket No. 23-119 (Rel. Apr. 25, 2023), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/104251437004710. The Proposed Rule was published in the Federal Register at 88 Fed. Reg. 50,846 (Aug. 1, 2023) and is available at https://www.federalregister.gov/documents/2023/08/01/2023-13040/review-of-international-authorizations-to-assess-evolving-national-security-law-enforcement-foreign [hereinafter "NPRM"].

[2] Electronic Privacy Information Center, https://epic.org/.

[3] *See in re* Implementation of the Telecommunications Act of 1996: Petition for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information, EPIC Petition, CC Docket No. 96-115 (Oct. 25, 2005), https://www.fcc.gov/ecfs/search/search-filings/filing/5513325075.

negligent data practices.[4] This advocacy is aligned with pillars one and three of the National Cybersecurity Strategy,[5] which call for stronger minimum cybersecurity requirements to defend critical infrastructure and for privacy and data security practices that drive security and resilience.

In these reply comments, EPIC emphasizes the threats to American communications infrastructure in terms of security, civil liberties, and economic activity; urges the Commission to require meaningful certifications of compliance with baseline cybersecurity measures; supports a regime in which required effort scales with risk; and encourages annual recertification of both cybersecurity and general legal compliance information. EPIC also supports the use of the Commission's 201(b) and 4(i) authority and refutes challenges offered by commenters based on an alleged lack of organic Commission authority, an alleged lack of authority in view of the Major Questions doctrine and the Congressional Review Act, and the contention that the proposed rule is both overinclusive and underinclusive.

II. Cybersecurity and Data Privacy Threats Demand Commission Action.

As many as half of U.S. consumers have been affected by data breaches because a company holding their personal information was hacked.[6] That is significantly higher than the global average of just 33 percent of consumers.[7] Although it can be difficult to remedy the harms of account compromise and identity theft, in many cases preventing the underlying breach is neither difficult

[4] *See, e.g., In re* Empowering Consumers Through Broadband Transparency, Comments of CDT, EPIC, and Ranking Digital Rights, CG Docket No. 22-2 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/102161424008021; *In re* Location-Based Routing for Wireless 911 Calls, Comments of EPIC, PS Docket No. 18-64 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10216148603009; *In re* Rates for Interstate Inmate Calling Services, Letter Comment of EPIC, WC Docket No. 12-375 (Dec. 15, 2022) https://www.fcc.gov/ecfs/search/search-filings/filing/121545964412.

[5] *See* Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

[6] *See* Prof. Carsten Maple, *2022 Consumer Digital Trust Index: Exploring Consumer Trust in a Digital World* 9 (2022), available at https://cpl.thalesgroup.com/resources/encryption/consumer-digital-trust-index-report.

[7] *See id.*

nor expensive. The Department of Homeland Security has estimated that 85 percent of data breaches were preventable,[8] and more recently the Internet Society has estimated 95 percent of breaches could have been prevented.[9] The Federal Trade Commission (FTC) has brought multiple enforcement actions against companies for failing to implement readily-available low-cost security measures.[10] Despite these realities, earlier this year an IBM study reported that breached organizations were more likely to pass the cost of incidents on to consumers rather than invest in better cybersecurity practices.[11] This is not a sustainable model for a healthy marketplace.

The consequences of failing to safeguard consumer data are not merely financial and do not fall solely on individual consumers victimized by breaches. The National Telecommunications and Information Administration (NTIA) has emphasized that Americans are increasingly concerned about online security and privacy, reporting that 45 percent of American households have abandoned conducting financial transactions, posting on social networks, or expressing opinions on the internet

[8] *See* 37 Dep't of Homeland Sec. Comput. Emergency Readiness Team, TA15-119, *Alert: Top 30 Targeted High Risk Vulnerabilities* (2016), https://www.cisa.gov/news-events/alerts/2015/04/29/top-30-targeted-high-risk-vulnerabilities.

[9] *See* Internet Society's Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report* at 3 (July 9, 2019), https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf.

[10] *See, e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC, d/b/a CafePress*, FTC File No. 1923209 at ¶ 11(a), 11(i)(i) (Jun. 23, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter; Complaint, *In re SkyMed International, Inc.*, FTC File No. 1923140 at ¶ 23 (Jan. 26, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923140-skymed-international-inc-matter; Complaint, *In re InfoTrax Systems, L.C.*, FTC File No. 1623130 at ¶ 11 (Dec. 30, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3130-infotrax-systems-lc; Complaint, *In re LightYear Dealer Technologies, LLC*, FTC File No. 1723051 at ¶ 22 (Sept. 6, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3051-lightyear-dealer-technologies-llc-matter; Complaint, *FTC v. Equifax, Inc.*, No. 1:2019-cv-03297 at ¶¶ 23(A)(iv), 24 (N.D. Ga. Jul. 22, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc; Complaint, *FTC v. Ruby Life Inc. d/b/a AshleyMadison.com*, No. 1:16-cv-02438 at ¶¶ 23(A)(iv), 24 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3284-ashley-madison; Complaint, *In re Lenovo, Inc.*, FTC File No. 1523134 at ¶ 25 (Jan. 2, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3134-lenovo-inc.

[11] *See* IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs (July 24, 2023), https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs.

due to privacy and/or security concerns—and that 30 percent refrained from at least two of these activities.[12] PricewaterhouseCoopers and McKinsey have also cited to the priority consumers place on privacy and data security.[13] Pew Research Center has published multiple surveys underscoring the importance of privacy and documenting users feeling powerless and vulnerable due to companies failing to safeguard their data.[14] In 2022, VentureBeat summarized a Thales report as indicating that "more than one-fifth of consumers stopped using a company that experienced a data breach."[15] The Commission must take action to address this crisis in trust.

---

[12] *See* Rafi Goldberg, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, National Telecommunications and Information Administration, https://www.ntia.gov/blog/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (last visited Oct. 2, 2023).

[13] *See, e.g.*, PwC, Consumer Intelligence Series; Protect.me (2017), available at https://www.fisglobal.com/-/media/fisglobal/worldpay/docs/insights/consumer-intelligence-series-protectme.pdf ("88% say that their willingness to share their personal data is determined by how much they trust a company, and 87% will go elsewhere if they are given reason not to trust a business."); PwC, Are we ready for the Fourth Industrial Revolution?, https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/fourth-industrial-revolution.html (last visited Mar. 22, 2023) (64% of consumers want assurance of immediate notification if personal data is compromised); Venky Anant et al., The consumer-data opportunity and the privacy imperative, McKinsey & Company (Apr. 27, 2020), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative (noting that 12% consumers reported trusting telecom companies to protect their data as compared with 18% trusting retail companies, noting that 46% consumers reported that they trust companies that proactively report a hack or breach).

[14] *See, e.g.*, Kenneth Olmstead and Aaron Smith, Americans' experiences with data security, Pew Research Center (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/1-americans-experiences-with-data-security/ ("In total, around seven-in-ten cellphone owners are very (27%) or somewhat (43%) confident that the companies that manufactured their cellphones can keep their personal information safe; a similar share is very (21%) or somewhat (47%) confident that the companies that provide their cellphone services will protect their information…. At a broader level, roughly half (49%) of all Americans feel their personal information is less secure than it was five years ago."); Brook Auxier, et al, Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/ americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ ("81% of Americans think the potential risks of data collection by companies about them outweigh the benefits… Roughly seven-in-ten or more say they are not too or not at all confident that companies will admit mistakes and take responsibility when they misuse or compromise data"); Andrew Perrin, Half of Americans have decided not to use a product or service because of privacy concerns, Pew Research Center (Apr. 14, 2020), https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/ ("Overall, adults who experienced any of these three data breaches were more likely than those who did not to avoid products or services out of privacy concerns (57% vs. 50%).").

[15] *See* VB Staff, Report: 33% of global consumers are data breach victims via hacked company-held personal data, VentureBeat (Dec. 11, 2022), https://venturebeat.com/security/report-33-global-consumers-data-breach-victims-hacked-company-held-personal-data/.

Foreign actor access to Customer Proprietary Network Information (CPNI) and personally-identifiable information (PII) is a known priority for the Commission, as it can threaten not only confidentiality of consumer information but also implicate threats to the integrity of law enforcement efforts and national security interests.[16] Although EPIC maintains that all custodians of consumer data should be held to basic cybersecurity standards, we support the Commission's attention to international authorization holders as the first step towards implementing a more universal regulatory data privacy and data security regime.

Implementing baseline cybersecurity practices does not represent a burden to providers presently, and moreover does not represent an additional burden given the growing attention to cybersecurity and data privacy by state and federal regulators and by the White House. As noted in its comments in this proceeding, USTelecom found that "even our small members have a mature cybersecurity culture."[17] Even if that were not the case, regulations proposed by federal agencies

[16] *See in Re* China Unicom (Americas) Operations Ltd., FCC22-9, 2022 WL 354622, at *35–36 (F.C.C. Feb. 2, 2022) ("The Commission expressed concern in the *Institution Order* that CUA's service offerings provide CUA with access to both customer PII and CPNI, and that 'this access presents risks related to the protection of sensitive customer information and the effectiveness of U.S. law enforcement efforts'… Given the record evidence in this proceeding, we conclude that, as a provider of MVNO service, CUA has the opportunity to access CPNI, including CDRs, and that CUA may access at least some PII. This access provides opportunity to engage in activities that are harmful to the law enforcement and national security interests of the United States.") (internal citations omitted); *In re* P. Networks Corp. and Comnet (Usa) LLC, 37 F.C.C. Rcd. 6368 (F.C.C. 2021) ("In addition, Pacific Networks' and ComNet's service offerings provide them with access to personally identifiable information (PII) and CPNI concerning their customers, and this access presents risks related to the protection of sensitive customer information and the effectiveness of U.S. law enforcement efforts.").

[17] Comments of USTelecom at 4 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10831107732869 (citing to Cybersecurity Culture Report: The State of Small and Medium-Sized Critical Infrastructure Enterprises 4, USTelecom (Feb. 15, 2023), https://www.ustelecom.org/research/2023-cybersecurity-culture-report) ("The IT and Communications (Comms) sectors stood out as having he strongest cybersecurity cultures, with the Comms sector scoring most consistently high across the five dimensions. The IT, Comms, and Financial Services sectors were the most likely to perform important cybersecurity culture practices including performance appraisals, rewards for proactive behavior, training initiatives, and routine communications with internal stakeholders."). This last point about routine communications with internal stakeholders is important as other recent studies suggest some breaches might not even be reported internally. Press Release, Keeper Security Releases Cybersecurity Disasters Survey: Incident Reporting & Disclosure (Sept. 26, 2023), https://www.prnewswire.com/news-releases/keeper-

including the Securities and Exchange Commission,[18] the FTC,[19] and the Consumer Financial Protection Bureau,[20] as well as state regulators such as the California Privacy Protection Agency (CPPA)[21] underscore the increasing expectations placed on companies to safeguard the consumer data entrusted to their care. Moreover, earlier this year, the White House released its National Cybersecurity Strategy[22] and corresponding Implementation Plan, which together not only place expectations of minimum cybersecurity requirements on critical infrastructure sectors such as telecom companies but also consider how market forces can drive security and resilience across all sectors, including by promoting the privacy and security of personal data.[23] The cybersecurity status quo is no longer acceptable. Complaints from industry that this long-overdue change is somehow unexpected or burdensome should not hold the Commission back when so many other agencies are moving forward. Both federal agencies and consumers now rightly expect continuously vigilant and evolving cybersecurity and data security practices.

---

security-releases-cybersecurity-disasters-survey-incident-reporting--disclosure-301938319.html (noting that nearly half (48%) of the IT and security leaders in North America and Europe surveyed experienced a cybersecurity incident and did not report it to the appropriate external authorities, and that 41% of such attacks were not disclosed to internal leadership).

[18] *See* Press Release, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, 2023-139 (July 26, 2023), https://www.sec.gov/news/press-release/2023-139.

[19] *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (advanced notice issued Aug. 22, 2022), available at: https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

[20] *See* Press Release, CFPB Takes Action to Protect the Public from Shoddy Data Security Practices (Aug. 11, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-to-protect-the-public-from-shoddy-data-security-practices/.

[21] *See* California Privacy Protection Agency, Preliminary Rulemaking Activities on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking, https://cppa.ca.gov/regulations/pre_rulemaking_activities_pr_02-2023.html (last visited Oct. 2, 2023).

[22] *See* Fact Sheet note 5 *supra* (pillar one addresses defending critical infrastructure, pillar three addresses shaping market forces to drive security and resilience).

[23] The White House, National Cybersecurity Implementation Plan (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

The Commission's efforts in this rulemaking will help incentivize companies to invest in safeguards for the consumer data with which they have been entrusted. If greater protections are not implemented, multiple breaches each impacting tens or hundreds of millions of Americans will continue to occur every year.[24]

III. The Commission Should Enforce Adequately Independent, Thorough Audits that Align with Meaningful Cybersecurity Frameworks.

The Commission proposes to require applicants to certify that they will implement and adhere to baseline cybersecurity standards based on universally recognized standards like those provided by the National Institute for Standards and Technology (NIST).[25] The Commission also inquires about other recognized baseline cybersecurity standards and about whether the certification requirement should take into account the size of the applicant and its operations.[26] We urge the Commission to require meaningful certifications of compliance with baseline cybersecurity measures. Self-certification cannot satisfy this requirement unless (1) the audits being self-certified are not merely aligned with meaningful standards or frameworks but also are both independent and thorough, and (2) the Commission consistently brings enforcement actions against false or deficient certifications.

---

[24] *See, e.g.*, Press Release, Identity Theft Resource Center Sees Record-Setting Number of Data Compromises in Q2; On Pace to Set New Yearly Record, Identity Theft Resource Center (July 12, 2023), https://www.idtheftcenter.org/post/identity-theft-resource-center-sees-record-setting-number-of-data-compromises-q2-on-pace-new-yearly-record/ (also reporting T-Mobile as the largest breach in the first half of 2023); Bree Fowler, Data Breaches Break Record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/. Statista provides a graph of the number of reported data breaches dating back to 2005 (at which time there were 157); Statista Rsch. Dep't, Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2022, Statista (Jan. 2023), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/. For the telecom sector specifically, see, e.g., T-Mobile: Breach Exposed SSN/DOB of 40M+ People, Krebs on Security (Aug. 18, 2021), https://krebsonsecurity.com/2021/08/t-mobile-breach-exposed-ssn-dob-of-40m-people/. *See also* Comments of EPIC, *In re* Data Breach Reporting Requirements, WC Docket No. 22-21 (Feb. 23, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10222069458527.

[25] *See* NPRM at ¶ 99 https://www.federalregister.gov/d/2023-13040/p-197.

[26] *See id.* at ¶ 100 https://www.federalregister.gov/d/2023-13040/p-198.

It should not be difficult for the Commission to establish a meaningful minimum cybersecurity standard. There is striking similarity across multiple state laws, federal sectoral laws, FTC enforcement actions, and both government and non-government frameworks regarding basic modern cybersecurity hygiene.[27] Commenter critique that a framework such as the National Institute for Standards and Technology's (NIST's) is not a standard does not render adherence to that framework unreasonable or unfeasible;[28] as Verizon notes, the Tier 2 level of the latest version of NIST's Cybersecurity Framework (CSF) "provides an appropriate baseline."[29] Commenter challenges to the Commission's authority to set standards on the basis of a lack of expertise[30] similarly miss the point that the Commission can rely upon the expertise of others, such as NIST or the Center for Internet Security (CIS), even assuming (without conceding) that the Commission does lack such expertise.

Civil society organizations should continue to have a voice in the establishment of these standards, as industry interests are not aligned with consumer interests once a data breach results in litigation (and arguably earlier, at the point at which a company decides not to invest in better

[27] *See, e.g.*, Comments of EPIC to the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security 194-197 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM- comments-Nov2022.pdf; *see also* Comments of the Electronic Privacy Information Center, Center for Digital Democracy, and Consumer Federation of America, to the California Privacy Protection Agency, Proceeding No. 02-23 at Appendix 1 (Mar. 27, 2023), https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency/.

[28] *See, e.g.*, *in re* Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, Comments of Verizon, IB Docket No. 23-119, at 21-22 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/108312266504640; Comments of CTIA at 52 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/108311863500689; Comments of T-Mobile at 22-23 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10831234137677.

[29] Comments of Verizon at 23. Verizon goes on to say that "[a] Tier 2 baseline implementation of the CSF would thus serve as a dynamic, discerning, and risk-based approach consistent with the 2023 National Cybersecurity Strategy and the government's approach to cybersecurity as discussed above." Id. at 24-25. *See also* Comments of USTelecom at 10 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10831107732869.

[30] *See* Comments of Verizon at 8; Comments of CTIA at 26, 39, 54.

cybersecurity based on its own interests rather than the interests of its customers).[31] Industry policy priorities are also generally not aligned with consumer interests. For example, regulatory flexibility and harmonization can be at odds with timely and adequate protections for consumers. The need for flexibility in data security requirements ("no one-size fits-all") does not imply there should be no minimum threshold to ensure basic quality at all: this would be akin to arguing that because no single size fits everyone, we simply shouldn't have any sizes at all. Moreover, establishing a minimum baseline does not preclude the flexibility necessary to incorporate other standards that may be helpful in the future.[32]

Arguments that the Commission should wait for the Office of the National Cyber Director (ONCD) to conclude its harmonization efforts are also misplaced. The deadline for that Request for Information (RFI) is not until the end of October 2023,[33] and because the RFI is only an initial stage in any such effort, it is uncertain how long the process will take or even whether there will be an end result.[34] Consumers should not have to wait unreasonably long for basic cybersecurity protections. Concerns about harmonization can be better addressed by the National Security Telecommunications Advisory Council's recent guidance about agency regulations aligning towards consensus standards,[35] rather than by failing to implement any minimum safeguard standards.

---

[31] *See* IBM Report note 11 *supra*.
[32] *See, e.g.*, Comments of CTIA at 53.
[33] *See* Office of the National Cyber Director, Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations, 88 Fed. Reg. 55,694 (Aug. 16, 2023), https://www.federalregister.gov/documents/2023/08/16/2023-17424/request-for-information-on-cyber-regulatory-harmonization-request-for-information-opportunities-for.
[34] *See* Christian Vasquez, White House grapples with harmonizing thicket of cybersecurity rules, CyberScoop (Sept. 18, 2023), https://cyberscoop.com/cybersecurity-strategy-harmonization-critical-infrastructure/ ("That monumental task is likely to span years — perhaps even administrations. Its outcome has the potential to radically reshape cyber policy and regulations for 16 critical infrastructure sectors. Assuming it gets done.").
[35] *See* NSTAC Report to the President, Strategy for Increasing Trust in the Information and Communications Technology and Services Ecosystem at ES 5-6, 24, 25 (Feb. 21, 2023), https://www.cisa.gov/sites/default/files/2023-04/NSTAC_Strategy_for_Increasing_Trust_Report_%282-21-23%29_508_0.pdf.

Even use of appropriate standards will not result in meaningful certifications if the audits measuring adherence are not both independent[36] and thorough. As one example, an audit should not merely report the audit subject's response as to whether the organization has a strong password policy in place; rather, the auditor should actually attempt to set up access with a weak password to see if the policy has been implemented and works as intended.[37] Twitter whistleblower Peter "Mudge" Zatko remarked in Congressional testimony last year:

> "[H]ow was Twitter still operating like this? Since there was a 2011 consent decree that was aimed at addressing a fair amount of this? . . . One, there were a lot of evaluations and examinations, which were interview questions. So essentially, the organization was allowed to grade their own homework. Did you make things better? Yes, we did. Okay, check. There wasn't a lot of ground truth. There wasn't a lot of quantified measurements. And a fair amount of the interviews came from companies, auditors that Twitter themselves were able to hire. So I think that's a little bit of a maybe conflict of interest."[38]

Mudge suggested the solution include "accountability, and setting quantitative goals and standards that can be measured and audited independently" in order to "change management structures, and drive change in companies when it's needed such as this."[39] We urge the Commission to establish quantitative goals and standards, requiring actual investigation and analysis and not merely interviews.[40] We also encourage the Commission to establish processes that reduce the likelihood of

[36] We note that CTIA has also implied in its comments that internal audits should be independent to qualify as sufficient. *See* Comments of CTIA at 52.
[37] *See* Kevin G. Coleman, *Security Assessment or Security Audit?*, infoTECH Spotlight (Sept. 21, 2009), https://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm.
[38] Data Security at Risk: Testimony from a Twitter Whistleblower: Hearing Before the S. Comm. on the Judiciary, 117th Cong. (2022) (testimony of Peter Zatko), https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower.
[39] Id.
[40] Ultimately, the Commission's proposed rule only requires certification of adherence to an existing framework. We urge the Commission to state explicitly that a certification is deficient if the company's audit was based solely on staff interviews and did not entail any actual testing of whether the safeguards are operating as intended.

a conflict of interest as described in Mudge's testimony. CPPA has proposed measures that may be helpful to the Commission here.[41] Audits must be independent and thorough.

Bringing enforcement actions against entities filing false or deficient certifications will also be critical to the Commission achieving its goals in this proceeding. Unfortunately, false certifications about privacy and cybersecurity compliance are a known issue. The Department of Justice has set up an entire initiative to address this issue with regard to federal contractors.[42] Verizon has reported in the payment security context that the majority of organization fail to maintain compliance between annual compliance validations.[43] It would be wholly consistent for the Commission to bring enforcement actions related to inadequate data security practices for false or deficient certifications, as it has brought actions under Section 201(b) and more recently under 222 for failure to implement reasonable security measures to protect consumer information.[44]

[41] *See* Draft Cybersecurity Audit Regulations for California Privacy Protection Agency (CPPA) Sept. 8, 2023 Board Meeting, at 7-9 Section 7122, available at https://cppa.ca.gov/meetings/materials/20230908item8.pdf (last visited Oct. 2, 2023).

[42] *See, e.g.*, Press Release, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative; Madison Alder, Verizon agrees to settle False Claims allegations over cyber standards for federal contractors, FedScoop, (Sept. 5, 2023), https://fedscoop.com/verizon-to-settle-cyber-false-claims-allegations/.

[43] *See* Verizon, 2022 Payment Security Report 82 (Sept. 2022), https://www.verizon.com/business/resources/T38f/reports/2022-payment-security-report.pdf (Verizon consistently reports that 44 percent or more of organizations fail to maintain PCI- DSS compliance in between annual compliance validations (most recently more than 56 percent failed to maintain compliance).)

[44]*See, e.g.*, *In re* TerraCom Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175, at ¶ 12 (Oct. 24, 2014), https://docs.fcc.gov/public/attachments/FCC-14-173A1.pdf (provider failed to "employ reasonable data security practices to protect consumers' [Proprietary Information] PI" in violation of 201(b)) [hereinafter "2014 NAL"]. *See id.* at ¶ 1; *id.* at ¶¶ 33-34 (noting that "the Companies' data security practices created an unacceptable risk of unauthorized access" separate and apart from the breach of "approximately 128,066 proprietary records"). *See also In re* Q Link Wireless LLC and Hello Mobile Telecom LLC, Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-22-00034450, at ¶ 19 (July 28, 2023), https://docs.fcc.gov/public/attachments/FCC-23-59A1.pdf ("These practices plainly do not constitute reasonable data security measures and therefore violate both section 64.2010(a) of the CPNI rules and section 222 of the Act, which establishes carriers' duties for protecting customer information.") (internal citations omitted).

IV. Audits Should Be Risk-Based in Scope and Certifications Should Occur Annually.

Cybersecurity requirements should be set at a level commensurate with the scope and scale of the type and volume of data a company collects.[45] This will also incentivize companies to reduce the amount of data they collect, as they will have a bigger stake in the risks associated with collecting and retaining large volumes of data.[46] As such, we agree with CTIA that the extent of an audit should be risk-based and not solely size-based, although size may be a factor in a risk-based determination.[47] This risk-based approach has already been enacted as data security policy at the state level in at least one state,[48] and is likely to soon be enacted in California.[49]

Compliance with cybersecurity audits and with other laws and regulations should be certified annually, not every three years as the Commission proposes.[50] As noted above, organizations may fail to maintain compliance even between annual audits[51]—extending audits to every three years will only invite further risk of lapses in compliance between certifications. Regarding the Commission's

---

[45] *See, e.g.*, William McGeveran, The Duty of Data Security, 103 Minn. L. Rev. 1135, 1179 (2018), https://www.minnesotalawreview.org/wp-content/uploads/2019/02/1McGeveran_FINAL.pdf (noting that across multiple data security frameworks "the duty of data security scales up or down in proportion to the resources and risk profile of each data custodian").

[46] The FTC explicitly describes data minimization as a data security principle. *See* Trade Regulation Rule on Commercial Surveillance and Data Security note 19 *supra* at 51,277, available at: https://www.federalregister.gov/d/2022-17752/p-88. *See also* John Davisson, Data Minimization: A Pillar of Data Security, But More Than That Too (June 22, 2023), https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/.

[47] *See* Comments of CTIA at 53-54.

[48] *See, e.g.*, 201 Mass. Code Regs. 17.03(1) (2010), https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download (requiring a security program include "administrative, technical, and physical safeguards that are appropriate to: (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information").

[49] *See* CPPA Draft Cybersecurity Audit Regulations note 41 *supra* at 9 (Section 7123) ("(a) The cybersecurity audit shall assess and document the business's cybersecurity program that is appropriate to the business's size and complexity and the nature and scope of its processing activities, taking into account the state of the art and cost of implementation.")

[50] *See* NPRM at ¶ 129 https://www.federalregister.gov/d/2023-13040/p-240; id. at ¶ 98 https://www.federalregister.gov/d/2023-13040/p-196.

[51] *See* 2022 Payment Security Report note 43 *supra*.

proposals about reporting violations of other laws, regulations, or policies,[52] there is no reason to wait to report these violations every three years rather than aggregate reporting on annual basis.

V. Challenges to the Commission's Proposals Raised by Commenters Do Not Preclude Commission Action.

No arguments raised by commenters should prevent the Commission from moving forward with its proposals; however, we only directly address a few arguments here. EPIC supports the Commission's use of its 201(b) and 4(i) authority to implement this regulation to maintain consumer trust in our communications networks. Challenges offered by commenters based on an alleged lack of organic Commission authority, an alleged lack of authority in view of the Major Questions doctrine and the Congressional Review Act, and the contention that the proposed rule is both overinclusive and underinclusive are all unavailing. We address each in turn below.

a. The Commission's Proposals Fall Within the Scope of its Authority Under Sections 201(b) and 4(i).

The Commission has authority to implement its proposed rules under existing authorities without the need for action from Congress. In its NPRM, the Commission cites to its authorities under Sections 4(i), 201(b), and 214 of the Communications Act of 1934.[53] We agree that it has authority under Section 214 and argue further below that it has authority under 201(b) and 4(i).

For many years, and as recently as 2021,[54] the Commission has cited to 201(b) as a core data privacy and data security authority. For example, the Commission drew on its 201(b) authority in

[52] *See* NPRM at ¶ 33 https://www.federalregister.gov/d/2023-13040/p-68; id. at ¶ 130 https://www.federalregister.gov/d/2023-13040/p-241.
[53] *See* id. at ¶ 5, https://www.federalregister.gov/d/2023-13040/p-29.
[54] *See in re* Protecting Consumers from Sim Swap and Port-Out Fraud, 36 F.C.C. Rcd. 14120 n 66 (F.C.C. 2021) ("At the same time, we emphasize that carriers have statutory duties to protect the confidentiality of their customers' private information and to maintain just and reasonable practices and that these statutory duties are not necessarily coterminous with our rules. *See* 47 U.S.C. §§ 222(a), 201(b); *TerraCom, Inc., and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014). Recent breaches appear to demonstrate that current safeguards are not sufficient to protect consumers' data.").

two 2015 data protection-related enforcement actions[55] and in the 2014 NAL against TerraCom and YourTel.[56] Additionally, on multiple occasions Commissioner Starks has emphasized privacy and data security in matters grounded in the Commission's 201(b) authority.[57]

That section 201(b) confers privacy authority on the Commission is also apparent from the Federal Trade Commission's exercise of its analogous section 5 powers to regulate harmful commercial data practices. Section 5 of the FTC Act prohibits unfair or deceptive acts or practices,[58] including harmful data practices.[59] Section 201(b) of the Communications Act prohibits "any charge, practices, classification, or regulation that is unjust or unreasonable."[60] As the FTC can bring enforcement actions for Section 5 violations committed by companies that are not acting in their capacity as common carriers, so too can the Federal Communications Commission use its 201(b) authority to regulate harmful data practices by carriers. Both agencies have documented this

[55] *See in re* AT&T Services, Inc., 30 F.C.C. Rcd. 2808 at ¶ 2 (F.C.C. 2015) ("The failure to reasonably secure customers' personal information violates a carrier's duty under Section 222 of the Communications Act, and also constitutes an unjust and unreasonable practice in violation of Section 201 of the Act."); id. at ¶ 3 ("The Notice of Apparent Liability in *TerraCom* states that Section 201(b) applies to carriers' practices for protecting customers' PII and CPNI."); *In Re* Cox Commun., Inc., 30 F.C.C. Rcd. 12302 (F.C.C. 2015) ("Privacy Laws" means Sections 47 U.S.C. §§ 201(b), 222, and 551, and 47 C.F.R §§ 64.2001-2011, insofar as they relate to the security, confidentiality, and integrity of PI and/or CPNI.)").

[56] *See* 2014 NAL note 44 *supra*.

[57] *See, e.g., In re* Protecting Against Natl. Sec. Threats to the Commun. Supply Chain Through Fcc Programs, 35 F.C.C. Rcd. 7821 (F.C.C. 2020) ("untrustworthy equipment that threatens our data privacy and network security cannot be managed or tolerated in any form"). *See also, In re* Protecting Against Natl. Sec. Threats to the Commun. Supply Chain Through Fcc Programs Huawei Designation Zte Designation, 34 F.C.C. Rcd. 11423 (F.C.C. 2019) ("…I have said many times that the untrustworthy equipment from these companies could readily serve as a 'front door' for Chinese intelligence gathering, at the expense of our privacy and national security.").

[58] 15 U.S.C. § 45(a)(1) (2018).

[59] *See, e.g.*, First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015), https://www.ftc.gov/legal-library/browse/cases-proceedings/1023142-x120032-wyndham-worldwide-corporation (failing to maintain reasonable and appropriate data security); Complaint, FTC v. Twitter, Inc., Case No. 3:22-cv-03070 (N.D. Cal. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023062TwitterFiledComplaint.pdf (collecting phone numbers purportedly for security purposes but then using those phone numbers for advertising purposes); Complaint, In re Support King, LLC, FTC File No. 1923003 (Dec. 21, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3003-support-king-llc-spyfonecom-matter (licensing, marketing, and selling stalkerware app).

[60] 47 U.S.C. § 201(b).

understanding of their analogous authorities in a 2016 Consumer Protection Memorandum of Understanding (CP MOU) between the Commission and the FTC, which articulates that the two agencies "will continue to work together to protect consumers from acts and practices that are deceptive, unfair, unjust and/or unreasonable."[61] The CP MOU additionally notes that "no exercise of enforcement authority by the FTC should be taken to be a limitation on authority otherwise available to the FCC" (and vice versa), and that "[t]o the extent that existing law permits both the FCC and the FTC to address the same conduct, the agencies agree to follow [the CP MOU] to ensure that their activities efficiently protect consumers and serve the public interest."[62] The agencies clearly (and correctly) contemplate parallel authority between Section 5 and Section 201(b). This includes authority to protect consumers from unjustly or unreasonably deficient cybersecurity practices.

Section 4(i) clearly authorizes the Commission to "perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this Act, as may be necessary in the execution of its functions."[63] This includes the revocation of authorizations where providers are no longer acting in the public interest, especially where providers have allowed for the kind of reduction or impairment in service represented by deficient cybersecurity practices.

More broadly, ever since the *Carterfone* decision more than 50 years ago the Commission has had the authority to police the interface between the network and end-user hardware.[64] Service provider facilities and hardware that receive data from and transmit data to end-user devices (if only

[61] FCC-FTC Consumer Protection Memorandum of Understanding 1 (Nov. 16, 2015), https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1116/DOC-336405A1.pdf [hereinafter "CP MOU"].
[62] CP MOU at 2.
[63] 47 U.S.C. § 154.
[64] Kevin Werbach explains this in The Federal Computer Commission, 84 N.C. L. Rev. 1, 5 (2005), available at: https://scholarship.law.unc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=4184&context=nclr (citing to Use of the Carterfone Device in Message Toll Telephone Services, 13 F.C.C. 2d 420 (1968), recon. denied, 14 F.C.C. 2d 571 (1968)).

indirectly) clearly fall within the ambit of this well-established Commission authority, especially where the privacy or security of end-user data is concerned.

b. Challenges Based Upon the Major Questions Doctrine and the Congressional Review Act Necessarily Fail.

Some commenters have raised challenges to this rule based in the Major Questions doctrine or the Congressional Review Act—these arguments cannot succeed because the Supreme Court has already explicitly noted that Section 201(b) is an adequate delegation of authority to the Commission and because the scope and factual context of this proposed rule are different from the proposed 2016 rule that was subject to the joint resolution of disapproval.

The Major Questions doctrine entails an inquiry as to whether Congress clearly empowered the agency with authority over an issue that has vast economic and political significance.[65] Here, the Commission is proposing to require providers to certify that they are meeting basic minimum cybersecurity standards when handling consumer data. As we note above,[66] the Commission is not an outlier at the vanguard of this policy change. Several other federal agencies have already implemented or signaled intent to implement similar regulations designed to improve data privacy and security for consumers.[67] Moreover, the White House has established that improving cybersecurity for critical infrastructure sectors and strengthening privacy protections across all sectors are essential to its National Cybersecurity Strategy. While EPIC believes such changes will be significant to consumers in economic and non-economic ways, it would be a stretch to argue that against such a backdrop, the Commission's proposed cybersecurity regulations uniquely present issues of vast economic and political significance. Even if a court were to find this to be an

[65] *See* Kate R. Bowers, Cong. Research Serv., IF12077, The Major Questions Doctrine (updated Nov. 2, 2022), https://crsreports.congress.gov/product/pdf/IF/IF12077.
[66] *See* Section II, *supra*.
[67] *See* id.

extraordinary exercise of authority, Congress clearly intended for the Commission to require providers to protect consumer data under Section 201(b), as we argue above.[68] The Supreme Court has literally cited to Section 201(b) as an example of a clear grant of authority by Congress "because the statute gives an agency broad power to enforce all provisions of the statute" and juxtaposed it with a different agency's assertion of regulatory authority at issue in the case which the Supreme Court rejected.[69] Major Questions arguments are a waste of ink where Section 201(b) applies.

The Congressional Review Act (CRA) prohibits an agency from issuing a rule that is substantially the same as one subject to a joint resolution of disapproval.[70] According to the Congressional Research Service, two rules have been reissued following disapproval; both agencies focused on changing the aspects of the rule related to Congress's specific objections, as indicated by the legislative history.[71] CRA-based challenges to the Commission's proposals would first need to show that the current regulation is substantially the same as a regulation that was subject to a joint resolution of disapproval.[72] While data security provisions to protect consumer information were a part of the Commission's 2016 rule which was subject to CRA disapproval, it was only one small piece out of many,[73] meaning this rule does not have substantially the same scope.[74] Moreover, even

[68] *See* Section V(a), *supra*.
[69] *Gonzales v. Oregon*, 546 U.S. 243, 259 (2006) (citing to *Natl. Cable & Telecomm. Ass'n v. Brand X Internet Services*, 545 U.S. 967, 980 (2005)).
[70] *See* Maeve P. Carey and Christopher M. Davis, Cong. Research Serv., IF10023, The Congressional Review Act (CRA): A Brief Overview (updated Feb. 27, 2023), https://crsreports.congress.gov/product/pdf/IF/IF10023.
[71] *See id.* at 2.
[72] Most likely the Commission's 2016 Rule, "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services" 81 Fed. Reg. 87,274 (December 2, 2016), subject to disapproval in Pub. L. No. 115-22 (Apr. 3, 2017), available at: https://www.govinfo.gov/content/pkg/PLAW-115publ22/pdf/PLAW-115publ22.pdf.
[73] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274 (Dec. 2, 2016), available at: https://www.federalregister.gov/documents/2016/12/02/2016-28006/protecting-the-privacy-of-customers-of-broadband-and-other-telecommunications-services.
[74] *See, e.g.*, Comments of EPIC, *In re* Data Breach Reporting Requirements, WC Docket No. 22-21 at 12-13 (Feb. 23, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10222069458527 (citing to Comments of the Rural Wireless Association, Inc., WC Docket No. 21-341 at 7-11 (filed Nov. 15, 2021),

if the scope of the proposed rule was identical, the factual predicates are different now.[75] As EPIC and others have argued before, the threat landscape has become much worse than it was in 2016.[76] The DOJ and NTIA have additionally noted: "the national security landscape has changed since the FCC initially granted these authorizations [in 2007]."[77]

As a policy matter, Congress has thus far been unable to pass a comprehensive privacy law. Consumers need protection now. Here, the Commission is not mandating specific actions but rather permitting compliance with one of a number of frameworks that recommend basic minimum safety standards to protect consumer data.

c. Risk-Based Auditing Mitigates Over-inclusivity, Articulating the Scope of Immediate Commission Priorities Mitigates Under-inclusivity.

We disagree that the Commission's proposal is overinclusive or underinclusive—assuming, at least, the Commission takes a risk-based approach and articulates that this rule reflects prioritization and not the Commission's last word on cybersecurity. Verizon argues that the NPRM's reporting proposals are overinclusive because they would apply to providers who do not pose any articulable risk[78] and are underinclusive because they do not apply to other key components in the internet ecosystem.[79] As noted above,[80] EPIC supports a risk-based approach to the robustness required of audits; however, it is no great burden for a company to certify what measures it has

https://www.fcc.gov/ecfs/search/search-filings/filing/11151940542 99 (noting DOL rule disapproved under CRA later resubmitted with a different scope and unchallenged by Congress, arguing prevalence of data breaches has become endemic problem within telecom industry within recent years, and citing to statement of Rep. Blackburn that the Commission should not encroach upon the FTC's privacy jurisdiction)).

[75] See id.

[76] *In Re* Data Breach Reporting Requirements, Reply Comments of EPIC, Center for Democracy and Technology, Privacy Rights Clearinghouse, and Public Knowledge, WC Docket No. 22-21 at 13-15 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814.

[77] Comments of NTIA and DOJ at 1 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10412564521934.

[78] *See* Comments of Verizon at 2-3.

[79] *See id.* at 3, 22.

[80] *See* Section IV *supra*.

undertaken (including minimal measures in instances of minimal articulable risk). We agree that the Commission should require all entities subject to its jurisdiction to implement basic minimum cybersecurity requirements, not merely 214 authorization holders and applicants. However, this rulemaking is not counterproductive to that end goal and reflects a sensible prioritization by the agency given the interests at stake.

VI. Conclusion

We again applaud the Commission's attention to the increasingly severe and largely avoidable impacts of data breaches on American consumers; we support the Commission's use of meaningful audits and timely, accurate certifications to incentivize companies to improve their data security practices; and we reiterate the importance of strengthening the overall security of America's networks and protecting consumers from the harms of breaches.

Respectfully submitted, this the 2nd day of October 2023, by:

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036
frascella@epic.org