FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Safeguarding and Securing the Open Internet	)	WC Docket No. 23-320
	)	
	)	

Relating to the
Notice of Proposed Rulemaking
Released October 20, 2023

Reply Comments of Electronic Privacy Information Center

January 17, 2024

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

Table of Contents

Comments

I. Introduction and Summary

The **Electronic Privacy Information Center**[1] files these reply comments regarding the issues raised in the Notice of Proposed Rulemaking (NPRM) regarding "Safeguarding and Securing the Open Internet" issued on October 20, 2023.[2] We re-iterate the urgent need for the Federal Communications Commission ("FCC" or "Commission") to use its Title II authorities to protect users of broadcast services from misuse of their personal data. Sections 201(b) and 222 authorities in this context would empower the Commission to impose duties on internet service providers (ISPs) to safeguard the information of consumers—including but not limited to customer proprietary network information (CPNI)—and to promulgate rules that prohibit unjust and unreasonable practices more broadly. In short, we recommend that the Commission:

- Articulate how its authorities under Sections 201(b) and 222 are capable of regulating privacy and cybersecurity protections for consumer data beyond the data types listed in Section 222(h);
- Articulate how its authority is parallel and complementary with that of the Federal Trade Commission (FTC), and note that some responsibilities may be different for ISPs than for edge providers;
- Find that consumer privacy and data security harms outweigh purported regulation-induced revenue losses of advertisers;
- Resume immediately its consumer privacy and data security rulemaking; and
- Continue to facilitate cooperation with the FTC and State attorneys general (AGs) in combatting fraud.

[1] EPIC 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, has played a leading role in developing the Commission's authority to address emerging privacy and cybersecurity issues, and routinely advocates before the Commission for rules that protect consumers from exploitative data practices.

[2] *In re* Safeguarding and Securing the Open Internet, WC Dkt. No. 23-320 (Rel. Oct. 20, 2023), https://docs.fcc.gov/public/attachments/FCC-23-83A1.pdf. The Proposed Rule was published in the Federal Register at 88 Fed. Reg. 76,048 (Nov. 3, 2023) and is available at https://www.federalregister.gov/documents/2023/11/03/2023-23630/safeguarding-and-securing-the-open-internet.

In Section II of our comments, we further address the scope of Section 222 in response to commenters. In Section III, we refute claims that it is arbitrary and capricious to regulate ISPs but not edge providers, especially as relates to privacy and cybersecurity. In Section IV, we respond to claims that purported market harms should take priority over actively-occurring consumer harms. In Section V, we further address the need for an immediate rulemaking on privacy and cybersecurity. In Section VI, we encourage the Commission to continue to work with the Federal Trade Commission (FTC) and State AGs on matters of robocalls, robotexts, and other online fraud issues.

II. Sections 201(b) and 222 are capable of safeguarding consumer data because they cover broader types of information than those explicitly listed in Section 222(h).

Several commenters have raised questions about the scope of Section 222, noting that aspects of data generated by usage of Broadband Internet Access Service ("BIAS") such as metadata, the actual content an end-user views,[3] and deep packet inspection[4] may fall outside its scope. As we noted in our initial comments in this docket,[5] the Commission's authority under Title II is not limited to its CPNI authority, but also includes its authority under Section 222 governing non-CPNI customer proprietary information and personally identifiable information (PII) under Section 222(a), and Section 201(b) authorizes the Commission to prohibit any practices it finds to be unjust or unreasonable. The Commission has ample authority under Title II, even setting aside its authorities under Section 201(b) to address privacy and data security deficiencies, to safeguard consumer information under Section 222. The Commission's privacy

[3] *See* Comments of Computer & Communications Industry Association at 17 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/121461569394 ("There are aspects of BIAS, however, that have no true analog in traditional telephony, such as metadata, or are outside the bounds of what Section 222 governs, such as the actual content an end user views. The Commission should be clear in the extent to which Section 222 will apply to BIAS, choosing only the 'information' that is a clear analog to the non-BIAS telecommunications service information that the Commission is charged with protecting.").

[4] *See* Comments of Children's Health Defense at 2 (Nov. 20, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1120904016023 ("This definition of CPNI does not fully translate into the broadband internet access environment because it fails to account for information the carrier may obtain as a result of the carrier/customer relationship. BIAS providers routinely employ deep packet inspection and can otherwise discern content and other higher layer information that cannot be easily characterized as 'technical configuration, type, destination, location, [or] amount of use.' Nonetheless, it is sensitive and personally-identifying – and often privacy implicating. Stated simply, there is some personal and private information carriers obtain that technically does not constitute CPNI under the current definition.").

[5] *See* Comments of EPIC, Public Knowledge, Consumer Federation of America, and Demand Progress Education Fund at Section II(b) (Dec. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1215730424019 [hereinafter "Comments of EPIC et al."].

authority extends beyond CPNI to any kind of consumer information that "a customer would normally wish to protect,"[6] as well as to any PII.[7]

III. Regulating ISPs without regulating edge providers is not arbitrary and capricious, especially with regards to privacy and data security.

Several commenters have claimed that it would be arbitrary and capricious (or otherwise inadvisable) for the Commission to impose Title II requirements on ISPs while leaving larger tech companies, such as social media platforms, subject to the Federal Trade Commission's (FTC's) Section 5 authority.[8] Taking this position is tantamount to arguing that a phone carrier shouldn't have any obligation to protect a subscriber's device location data as CPNI because it would be arbitrary and capricious for apps a user runs on their handset to be subject to FTC Section 5 regulation at the same time that the Commission regulates a carrier's own use of the same or similar data. This is precisely the state of things[9] for phone carriers, and there is no reason a similar partnership between the Commission and the FTC can't apply to ISPs as well. We note however the FCC's laggard pace in enforcing existing protections for subscriber

[6] *See, e.g.*, *In re* Quadrant Holdings LLC, Q Link Wireless LLC, and Hello Mobile LLC, 202232170008, 2022 WL 3339390, at *7 n 25 (F.C.C. Aug. 5, 2022).

[7] *See, e.g.*, *In re* P. Networks Corp. and Comnet (Usa) LLC, FCC22-22, 2022 WL 905270, at *72 n 459 (F.C.C. Mar. 23, 2022) (citing to *In re* TerraCom Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175 (Oct. 24, 2014)) ("[PII is] information that can be used on its own or with other information to contact, or locate a single person, or to identify an individual in context."). On several occasions, the Commission has re-iterated that all communications service providers have a statutory responsibility to protect customer information, including PII and CPNI. *See id.* at *37 ¶ 82; *In re* Data Breach Reporting Requirements, Report and Order, WC Docket No. 22-21 (Rel. Dec. 21, 2023) at ¶ 75 n. 304, *available at* https://docs.fcc.gov/public/attachments/FCC-23-111A1.pdf (citing to *id.* and to China Telecom (Americas) Corporation, Order on Revocation and Termination, FCC 21-114, 36 FCC Rcd 15966, 16013-14, ¶ 72 (2021), *aff'd*, China Telecom (Americas) Corporation v. FCC, 57 F.4th 256 (D.C. Cir. 2022)).

[8] *See, e.g.*, Comments of CTIA at 86 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1214144547233; Comments of the Free State Foundation at 44-45 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1214009701346; Comments of NTCA-the Rural Broadband Association at 26 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/121458348415; Comments of WISPA-Broadband Without Boundaries at 93 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/121440645853; Comments of NCTA- The Internet & Television Association at 48-49, 57, 61 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/121484978453 [hereinafter "NCTA Comments"].

[9] *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data; Press Release, Fed. Trade Comm'n, Android Flashlight App Developer Settles FTC Charges It Deceived Consumers (Dec. 5, 2013), https://www.ftc.gov/news-events/news/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived-consumers.

location data,[10] including referring matters to other agencies in a less than timely and effective manner.[11]

In both the phone context and the ISP context, the FCC oversees the misuse of the underlying communications infrastructure by consumer-facing service providers, whereas the FTC only concerns itself with businesses offering their products and services by means of that infrastructure. The sister agencies recognize one another's strengths via MOU, the FTC in consumer protection and the Commission in consumer protection as applied to telecommunications services.[12] Moreover, as we have discussed in the Commission's docket on data breach reporting requirements, there is a clear parallel structure between the FTC's Section 5 authority and the Commission's authority under 201(b) articulated in a Memorandum of Understanding (MOU) between the two agencies,[13] suggesting harmonization of regulation and mitigating concerns that over the top (OTT) providers will be somehow subject to an entirely different regulatory regime than ISPs. However, some differences may be appropriate—the White House has emphasized the importance of more capable actors in cyberspace bearing greater responsibility for cybersecurity,[14] for example, which includes critical communications infrastructure such as ISPs.

---

[10] *See* FCC Proposes Over $200M in Fines for Wireless Location Data Violations (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations. The four-years-long lack of follow-through on this NAL has been pointed to by some commenters as indicative of a lack of Commission authority. *See, e.g.*, Ex Parte, CTIA, *In re* Protecting Consumers from SIM Swap and Port-Out Fraud, WC Docket No. 21-341 at 13 (Nov. 8, 2023), available at https://www.fcc.gov/ecfs/search/search-filings/filing/1109425224347 ("Proposed enforcement actions—such as the NAL that the Commission cites do not constitute final Commission orders and thus do not establish Commission precedent.").

[11] *See, e.g.*, *In re* AT&T Inc., File No.: EB-TCD-18-00027704, Statement of Comm'r Geoffrey Starks at 42 (Feb. 28, 2020), *available at* https://docs.fcc.gov/public/attachments/FCC-20-26A1.pdf ("But that is no excuse for failing to conduct a comprehensive investigation—including issuing subpoenas to Securus—of the events in question here. That information would have enriched our investigation and could have been provided to other agencies for investigation and enforcement.").

[12] *See* FCC-FTC Consumer Protection Memorandum of Understanding at 1 (Nov. 16, 2015), https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1116/DOC-336405A1.pdf [hereinafter "CP MOU"]. Note that a later (2017) MOU states that "nothing in this Memorandum should be construed as altering, amending, or invalidating [the 2015 CP MOU]." Restoring Internet Freedom: FCC-FTC Memorandum of Understanding at 1 n. 1 (Dec. 2017), https://www.ftc.gov/policy/cooperation-agreements/restoring-internet-freedom-fcc-ftc-memorandum-understanding.

[13] *See* Reply Comments of Electronic Privacy Information Center, Center for Democracy and Technology, Privacy Rights Clearinghouse, and Public Knowledge, *In re* Data Breach Reporting Requirements, WC 22-21 at 10-11 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814 (citing to CP MOU).

[14] *See* the White House, National Cybersecurity Implementation Plan 4 (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

In its comments, NCTA- The Internet & Television Association goes beyond concerns about agencies acting in parallel complicating regulatory harmonization, and claims that there is "no evidence of abusive practices by ISPs in the more than half-decade since the 2018 Order's release",[15] as if the FTC's 2021 Staff Report did not address the actual (not merely potential) privacy-related misconduct of ISPs.[16] NCTA's comment also argues that because there are greater cyber vulnerabilities in other parts of the internet ecosystem (e.g. cloud-based software), there is no basis for the Commission to seek to regulate the cybersecurity of broadband providers.[17] Even if counterfactually NCTA could demonstrate that there have been no vulnerabilities among ISPs, the risk of novel threat vectors could still demand regulatory action—in reality however, breaches of email content alone suggest immediate regulatory action must be taken to compel ISPs to shore up their cybersecurity practices to better protect consumers.[18] For similar reasons, we disagree with INCOMPAS' assessment that "there is no demonstrated need for the FCC to further engage in developing new cybersecurity regulations in this proceeding."[19] The breadth of the challenge posed by the ease of connecting to and through existing and new networks and the vulnerabilities in hardware, software, devices, and services demands a concomitant obligation to educate and protect users and their interests as fully as possible. For all the noise about regulatory disharmony, there is remarkable consistency in data security regulations.[20] While we do not believe the Commission needs to go into the same level of detail that other regulators and enforcers have on cybersecurity, the Commission can and should serve a vital, stabilizing role in promoting the consensus and near-consensus measures that currently seem to best protect consumers from breaches and other cyber incidents.

[15] NCTA Comments at 50.
[16] *See, e.g.*, Fed. Trade Comm'n, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* 33-44 (2021), *available at* https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major- internet-service-providers [hereinafter "FTC ISP Report"].
[17] NCTA Comments at 58-59.
[18] *See, e.g.*, Comments of EPIC et al. at 4 n. 15. Other ISP breaches are also relevant. *See, e.g., id.* at 4 n. 14.
[19] Comments of INCOMPAS at 28 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1214097190544.
[20] *See, e.g.*, Comments of EPIC and Consumer Reports, *In re* Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations, ONCD-2023-0001 at App'x 1 (Oct. 31, 2023), *available at* https://epic.org/documents/in-re-opportunities-for-and-obstacles-to-harmonizing-cybersecurity-regulations-rfi/.

IV. The Commission should find that consumer privacy and data security harms deserve greater weight than the hypothetical revenue losses of targeted advertising companies attributed to regulation.

Some commenters point to the economic gains from exploitation of consumer data, and the corresponding losses that would result if companies were forced to prioritize privacy and data security over the revenue generated by targeted advertising, as a reason for the Commission not to extend Title II authorities to BIAS.[21] As the FTC's ISP report explains: "As the internet assumes an increasingly pervasive role in the most personal aspects of our lives, including telehealth and distance learning, the aggregation of data—along with the privacy of consumer data in general—requires increased attention, especially for minority and low-income communities."[22] And as Bruce Schneier explains: the market does not reward healthy security.[23] To this point, two professors at Antonin Scalia Law School have similarly called out the failure of firms to internalize the costs and benefits of their data security decisions.[24] A key pillar of the National Cybersecurity Strategy is shaping market forces to drive security and resilience, making our digital ecosystem more trustworthy, including by "[p]romoting privacy and the security of personal data";[25] further emphasizing that this is not something that market forces will self-correct.

Alongside the FTC, the FCC is one of America's chief privacy regulators. The Communications Act of 1934 charges the Commission with protecting communications services subscribers' privacy.[26] As noted above, the FTC recognizes the Commission's particular expertise in consumer protection as applied to communications markets and infrastructure.[27] The

[21] *See, e.g.*, Comments of Privacy for America at 3, 4 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/12141195211758 at 3, 4; Comments of NCTA at 62 (astonishingly claiming without enumerating further that "[m]arket forces, backed by an array of existing statutory provisions and regulations, are more than sufficient to protect consumers").
[22] FTC ISP Report at 2.
[23] *See* Comments of EPIC et al. at 5 n. 18 (citing to Bruce Schneier, *The Uber Hack Exposes More Than Failed Data Security*, The New York Times (Sept. 26, 2022), https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html).
[24] *See* James C. Cooper & Bruce H. Kobayashi, Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem, 28 Mich. Tech. L. Rev. 257, 263–64 (2022), https://repository.law.umich.edu/mtlr/vol28/iss2/3.
[25] Fact Sheet, The White House, 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/ (Pillar Three- Shape Market Forces to Drive Security and Resilience).
[26] *See, e.g.*, 47 U.S.C. § 151 (creating Commission and charging it with executing and enforcing provisions including 47 U.S.C. § 222 which governs privacy of consumer information); CP MOU at 1.
[27] *See* CP MOU at 1.

FCC should find that privacy- and data security-related harms to consumers outweigh the purported benefits of invasive and pervasive data collection.[28] We further note that in the continuing absence of a comprehensive federal privacy law, if the Commission falls short in its responsibilities to protect consumer data collected by communications services providers, states will be left to correct the problem in a patchwork manner.

As a secondary matter, it's unclear that targeted advertising even accrues significant benefits to the advertisers themselves. A 2019 study found that targeted ads only marginally increase revenue;[29] other studies and polls suggest that behavioral ads perform worse than contextual ads which do not require consumer data collection.[30] While the Commission should base its finding on the harms to consumers rather than on the lackluster performance of the market segment, we do think it notable that the actual business impact of the surveillance economy is relatively unimpressive.

V. The Commission can immediately continue its existing consumer privacy and data security rulemaking.

If the Commission finalizes the proposed reclassification, it can and should move forward immediately from its 2016 Notice of Proposed Rulemaking (NPRM) on privacy and data security,[31] perhaps updating the factual record to better reflect the realities of 2024. Because the Commission interpreted the 2017 Congressional Review Act joint disapproval resolution of its

[28] *See, e.g.*, FTC ISP Report *supra* note 16.

[29] *See, e.g.*, Keach Hagey, Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests, Wall Street Journal (May 29, 2019), https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195 (noting study by researchers at the University of Minnesota, University of California, Irvine, and Carnegie Mellon University suggesting publishers only get about 4% more revenue for an ad impression that has a cookie enabled than for one that doesn't).

[30] *See, e.g.*, Ronald Gabriel, Behavioral Advertising vs. Contextual Advertising: What's the Difference? (last updated Jan. 3, 2022), https://martech.zone/behavioral-advertising-vs-contextual-advertising/ ("Contextual targeting averaged a 73% increase in performance when compared to behavioral targeting."); Brook Shepard, The New Rise of Contextual Advertising, Forbes (July 22, 2021), https://www.forbes.com/sites/forbesagencycouncil/2021/07/22/the-new-rise-of-contextual-advertising/?sh=71a687375e5d (noting poll by Digiday of publishing executives found that 45% of them saw no significant benefit from behavioral ads, and 23% said they actually caused a decline in revenue); Jack Neff, Nearly Half the Data Used for Ad Targeting is Wrong, AdAge (Oct. 10, 2023), https://adage.com/article/measurement/nearly-half-data-used-ad-targeting-wrong-truthset-study/2521136.

[31] *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, WC Dkt. No. 16-106 (Apr. 1, 2016), *available at* https://www.fcc.gov/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy.

2016 privacy rules order as rendering the order itself a nullity,[32] that would mean the docket the order was designed to complete could be developed immediately upon Title II classification without the need to initiate a new rulemaking. To those who would raise the specter of a Congressional Review Act (CRA) challenge to such a notion, we point out that the proposals in the 2016 NPRM differ from the Report and Order ultimately adopted,[33] and further note that the factual context under which the final rule was subject to a 2017 joint disapproval differs so significantly from the current data privacy and security context that even if the text of the rule itself was identical, the CRA would still not bar such a regulation.[34]

Some commenters note that there would be an enforcement vacuum for ISP-related abuses during the gap between Title II reclassification and implementation of a privacy rule, as the former would strip the FTC of its jurisdiction and the Federal Communications Commission would need to wait for the latter to take effect before it could take action.[35] This is wrong for at least two reasons. First, immediately upon being classified as a Title II service, ISPs would be subject to Sections 201(b) and 222 of the Communications Act. Enforcement penalties may differ after a separate privacy rule has taken effect, and a privacy rule may expand what conduct gives rise to liability, however there is nothing stopping the Commission from issuing Notices of Apparent Liability to ISPs on the first day of reclassification if on that day ISPs are still engaging in misconduct that violates those provisions of Title II. Second, the MOU between the Commission and the FTC indicates that the two agencies will "coordinat[e] on agency initiatives where one agency's action will have a significant effect on the other agency's authority or programs" and "consul[t] on investigations or actions that implicate the jurisdiction of the other agency."[36] This strongly suggests that any investigations conducted by the FTC prior to the

[32] *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Order, 32 FCC Rcd 5442 at ¶ 2 (Rel. June 29, 2017), *available at* https://digital.library.unt.edu/ark:/67531/metadc1225762/m1/875/?q=32%20FCC%20Rcd%205442 ("Because Pub. Law 115-22 was adopted pursuant to the Congressional Review Act, 5 U.S.C. § 801(f) provides that the 2016 Privacy Order 'shall be treated as though [it] had never taken effect.' ").
[33] *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Report and Order, WC Dkt. No. 16-106 (Nov. 2, 2016), *available at* https://docs.fcc.gov/public/attachments/FCC-16-148A1.pdf.
[34] *See* Comments of Electronic Privacy Information Center, *In re* Data Breach Reporting Requirements, WC 22-21 at 13 n. 50 (Feb. 22, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10222069458527.
[35] *See, e.g.*, Comments of NCTA at 69; Comments of ACA Connects – America's Communications Association at 33-34 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1214941413481.
[36] CP MOU at 1.

change in jurisdictional authority over ISPs would be shared with the Federal Communications Commission for follow-up.

VI. The Commission should work with the FTC and State AGs on robocall, robotext, and other online fraud issues.

We write here to echo comments that urge that the Commission and the FTC work together specifically to address online fraud.[37] Fraud is a perennial and growing problem,[38] and the agencies' historic partnership suggests that collaboration on this front could be fruitful.[39] We believe that a similar principle should apply to online fraud as to cybersecurity: the privilege of interconnection also confers an obligation to educate and protect users and their interests as fully as possible. Especially with the introduction of AI-supercharged scams[40] and scams tailored by breached data,[41] it is unreasonable to expect consumers to be equipped to protect themselves against the latest evolution of fraudster's schemes. Some financial services organizations for example have adjusted their one-time password text messages to better protect their customers.[42] The Commission should also continue to develop its partnerships with State attorneys general, who are often at the frontlines of scams targeting consumers.[43]

---

[37] *See, e.g.*, Comments of AARP at 8 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/12140625630149.

[38] *See, e.g.*, Press Release, Fed. Trade Comm'n, New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022, https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022 (noting nearly 2.5 million fraud reports and nearly $9 billion in reported losses); Fed. Trade Comm'n, Consumer Sentinel Network Data Book for January - December 2008 at 3 (Feb. 29, 2009), available at https://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2008/sentinel-cy2008.pdf (noting more than 600,000 fraud-related complaints and over $1 billion in consumer losses).

[39] *See, e.g.*, CP MOU.

[40] *See, e.g.*, EPIC, Generating Harms: Generative AI's Impact & Paths Forward at 2-3, 6, 66 (May 23, 2023), https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf; Alvaro Puig, Announcing the FTC's Voice Cloning Challenge (Nov. 16, 2023), https://consumer.ftc.gov/consumer-alerts/2023/11/announcing-ftcs-voice-cloning-challenge.

[41] *See, e.g.*, Press Release, Michigan Dep't of Att'y Gen., AG Nessel Reissues Consumer Alert Following New T-Mobile Data Breach (Jan. 24, 2023), https://www.michigan.gov/ag/news/press-releases/2023/01/24/ag-nessel-reissues-consumer-alert-following-new-t-mobile-data-breach.

[42] *See, e.g.*, HSBC UK customer warning: one time passcode fraud increases (Sept. 15, 2021), https://www.about.hsbc.co.uk/news-and-media/hsbc-uk-issues-customer-warning-as-one-time-passcode-fraud-increases ("HSBC UK customers will receive a warning in the SMS message containing their OTP instructing them to never share the code, even with bank staff or police.").

[43] *See, e.g.*, Press Release, Attorney General Josh Stein Leads New Nationwide Anti-Robocall Litigation Task Force (Aug. 2, 2022), https://ncdoj.gov/attorney-general-josh-stein-leads-new-nationwide-anti-robocall-litigation-task-force/; Press Release, Michigan Dep't of Att'y Gen., Attorney General Warns Gen Z May Be More Likely Scam Victims (Nov. 8, 2023), https://www.michigan.gov/ag/news/press-releases/2023/11/08/attorney-general-warns-gen-z-may-be-more-likely-scam-victims.

VII. Conclusion.

We appreciate the Commission's continued attention to consumer privacy and data security issues, and urge the Commission to act immediately to codify its Title II authority over ISPs accordingly.

Respectfully submitted, January 17, 2024.

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