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

Comments of

Electronic Privacy Information Center,
Public Knowledge,
Consumer Federation of America, and
Demand Progress Education Fund

December 14, 2023

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

Table of Contents

Comment

I. Introduction and Summary

The **Electronic Privacy Information Center**[1] and **Public Knowledge**,[2] along with **Consumer Federation of America**[3] and **Demand Progress Education Fund,**[4] file these comments regarding the questions raised in the Notice of Proposed Rulemaking (NPRM) on "Safeguarding and Securing the Open Internet" issued October 20, 2023.[5] We appreciate the Federal Communication Commission (Commission or FCC)'s efforts to protect consumer data from misuse by applying Title II of the Communications Act to broadband services. Extending the scope of the Commission's authorities under Sections 201(b) and 222 to broadband providers would enable the creation of stronger safeguards for consumers' personal information—included but not limited to customer proprietary network information (CPNI)—and support regulatory action to combat unjust and unreasonable practices online. These safeguards include three frameworks: CPNI under Section 222(h), non-CPNI privacy obligations under Section 222(a), and a general prohibition against unjust and unreasonable practices under Section 201(b).

In Section II of our comments, we outline what we expect Title II privacy protections would entail under three different frameworks and why immediate action by the Commission is so necessary. In Section III, we discuss the implications of Title II classification for robocalls and robotexts. We briefly address preemption in Section IV. In Section V, we urge the Commission to immediately commence a privacy and data security rulemaking. In Section VI,

[1] The Electronic Privacy Information Center (EPIC) is a public interest research center based in Washington, D.C. that was established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.
[2] Public Knowledge is a nonprofit advocacy group that promotes freedom of expression, an open internet, and access to affordable communications tools and creative works.
[3] The Consumer Federation of America (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.
[4] Demand Progress Education Fund is a 501(c)(3) charitable organization that educates the public about the perils of concentrated wealth and corporate power, the importance of maintaining an online ecosystem that allows for the flourishing of speech and democracy, and the value of diplomacy and respect for human and civil rights.
[5] *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 [hereinafter NPRM]. 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.

we discuss possible updates to the transparency rule required under the 2015 Open Internet Order.[6]

II. Title II offers multiple avenues for protecting consumer information, and timely application of Title II's protections is essential.

A lack of regulatory oversight has allowed not only economic and non-financial harms to befall consumers, but also exacerbated distrust in the network and had a chilling effect on online activity. Fortunately, Title II of the Communications Act gives the Commission broad authority to immediately address these problems: (1) through CPNI rules under Section 222(h); (2) through obligations to protect proprietary information and personally identifiable information under Section 222(a); and (3) through prohibitions on unjust or unreasonable practices under Section 201(b). We strongly support the Commission's efforts to subject broadband providers to Title II authority and encourage the Commission to take swift action to ensure that the privacy of users of broadband and other communications services is protected.

a. Timely protections are essential.

The Federal Communications Commission is a key federal privacy regulator, and the Commission's recent actions suggest an awareness of this reality and the urgency to act upon it.[7] The current landscape, the historic behavior of broadband and other telecommunications providers, and the need for immediate action in light of the limitations on the Federal Trade Commission's capacity all point to the need for the Commission to step in and assert the authority and expertise it has with respect to broadband service providers.

---

[6] Protecting and Promoting the Open Internet, WC Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5672-77, ¶¶ 162-70 (2015).

[7] *See, e.g.*, Fed. Commc'ns Comm'n, Privacy and Data Protection Task Force, https://www.fcc.gov/privacy-and-data-protection-task-force (last visited Dec. 13, 2023); FCC Fact Sheet, Data Breach Reporting Requirements, WC Docket No. 22-21 (Nov. 22, 2023), https://docs.fcc.gov/public/attachments/DOC-398669A1.pdf [hereinafter "FCC Data Breach Reporting Fact Sheet"]; *see also* Press Release, FCC Adopts Updated Data Breach Notification Rules to Protect Consumers (Dec. 13, 2023), https://www.fcc.gov/document/fcc-adopts-updated-data-breach-notification-rules-protect-consumers; FCC Enforcement Advisory, Telecommunications Carriers Must Protect Consumers' Privacy and Sensitive Data by Taking Reasonable Steps to Prevent SIM Fraud Schemes, DA 23-1148 (Rel. Dec. 11, 2023), https://docs.fcc.gov/public/attachments/DA-23-1148A1.pdf; Notice of Proposed Rulemaking, *In re* Cybersecurity Labeling for Internet of Things, PS Dkt. No. 23-239 (Rel. Aug. 10, 2023), https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-device.

The increasing prevalence of data breaches and large-scale privacy violations has raised the public's awareness of how their personal information is being mishandled and misused.[8] 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 due to privacy and/or security concerns—and that 30 percent refrained from at least two of these activities.[9] 63 percent of surveyed online households voiced concerns about identity theft, with 22 percent concerned about loss of control over personal data and 23 percent concerned with data collection by online services.[10] These numbers were elevated if the household had suffered a security breach in the year prior to the survey—for example, 70 percent were concerned about identity theft and 30 percent were concerned about data collection or tracking by online services.[11] As NTIA has reported, there is a clear connection between the strength of privacy and security safeguards on the one hand and healthy commerce and trust in American networks on the other hand. PricewaterhouseCoopers and McKinsey have also found

[8] *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/ ("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%).").

[9] *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 Dec. 13, 2023).

[10] *See id.*

[11] *See id.*

that consumers believe their privacy and data security are a high priority.[12] Pew Research Center has found that users consider privacy of their data to be of the utmost importance and that users feel powerless and vulnerable when companies fail to safeguard their data.[13]

These risks and concerns are not diminished in the context of telecommunications providers.[14] In the broadband industry, breaches can include hacked email accounts which in turn can expose the contents of communications as well as cryptocurrency accounts.[15] Moreover, normal market forces are unlikely to be able to correct for these cybersecurity deficiencies.[16]

---

[12] *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 Dec. 13, 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 consumer trust levels are "low overall", with the highest being 44% in healthcare and in financial services).

[13] *See* note 8 *supra.*

[14] *See, e.g.*, Jess Weatherbed, *Google Fi says customer data compromised by hackers*, The Verge (Feb. 1, 2023), https://www.theverge.com/2023/2/1/23580947/google-fi-mobile-tmobile-security-breach-data; SC Staff, *Charter Communications impacted by third-party breach*, SC Media a CyberRisk Alliance Resource (Jan. 30, 2023), https://www.scmagazine.com/brief/charter-communications-impacted-by-third-party-breach; Lawrence Abrams, *Cox discloses data breach after hacker impersonates support agent*, BleepingComputer (Dec. 9, 2021), https://www.bleepingcomputer.com/news/security/cox-discloses-data-breach-after-hacker-impersonates-support-agent/; Karl Bode, *An ISP Left Corporate Passwords, Keys, and All its Data Exposed on the Internet*, Vice (Oct. 23, 2018), https://www.vice.com/en/article/zm9dmj/an-isp-left-corporate-passwords-keys-and-all-its-data-exposed-on-the-internet; Daniel Stuckey, *Simple Website Flaw Exposed Data Of Charter Internet Customers*, *Fast Company* (May 20, 2015), https://www.fastcompany.com/3046477/simple-website-flaw-exposed-data-on-charter-internet-customers.

[15] *See, e.g.*, Lorenzo Franceschi-Bicchierai, *Hackers are breaking into email accounts to steal cryptocurrency*, TechCrunch (Apr. 26, 2023), https://techcrunch.com/2023/04/26/hackers-are-breaking-into-att-email-accounts-to-steal-cryptocurrency/; "Andrew-G", Looks like ISP email security has been compromised?, Virgin Media Community (Mar. 24, 2023, 08:25), https://community.virginmedia.com/t5/Email/Looks-like-ISP-email-security-has-been-compromised/td-p/5289195; Lawrence Abrams, *Comcast Xfinity accounts hacked in widespread 2FA bypass attacks*, BleepingComputer (Dec. 22, 2022), https://www.bleepingcomputer.com/news/security/comcast-xfinity-accounts-hacked-in-widespread-2fa-bypass-attacks/.

[16] Economics scholar Michael Kende—former Chief Economist of the Internet Society and Director of Internet Policy Analysis at the Commission, and current Senior Advisor at Analysys Mason and Visiting Professor at the Graduate Institute in Geneva—has similarly characterized the sorry state of cybersecurity and the resulting loss in digital trust as a consequence of three types of market failures: public goods, information asymmetry, and negative externalities. *See* Michael Kende, *How Secure Is Our Data,*

Internet service provider (ISP) customers in particular often face challenges that prevent them from changing providers in response to their dissatisfaction with inadequate data security, including contract periods and local monopolies.[17] Renowned security technologist and fellow at Harvard Kennedy School Bruce Schneier has emphasized this type of market failure:

> In all of these cases, the victimized organizations could have very likely protected our data better, but the reality is that the market does not reward healthy security. Often customers aren't even able to abandon companies with poor security practices, as many of them build "digital moats" to lock their users in. Customers don't abandon companies with poor security practices. Hits to the stock prices quickly recover. It's a classic market failure of a powerful few taking advantage of the many, and that failure is one that only representation through regulation can fix.[18]

Consumers fare no better when it comes to the protection of their privacy by telecommunications providers. A 2021 FTC Staff Report found that many broadband providers collect and then combine a host of individualized data about their customers across products, including the websites that customers visit, the shows they watch, the apps they use, details about their home energy use, their real-time and historical location, their internet search queries, and even the content of their communications.[19] Providers then use this broad array of data for

---

Really?, MIT Press Reader (May 16, 2021), https://thereader.mitpress.mit.edu/how-secure-is-our-data-really/.

[17] *See, e.g.*, Karl Bode, *Telecom monopolies are poised to waste the U.S.'s massive new investment in high-speed broadband*, Daily Dot (Jun. 30, 2022), https://www.dailydot.com/debug/broadband-telecom-monopolies-covid-subsidies/; Christopher Mitchell and Katie Kienbaum, *Report: Most Americans Have No Real Choice in Internet Providers*, Institute for Local Self-Reliance (Aug. 12, 2020), https://ilsr.org/report-most-americans-have-no-real-choice-in-internet-providers/; Emily Stewart, *America's monopoly problem, explained by your internet bill*, Vox (Feb. 18, 2020), https://www.vox.com/the-goods/2020/2/18/21126347/antitrust-monopolies-internet-telecommunications-cheerleading; Becky Chao, Claire Park, and Joshua Stager, *The Cost of Connectivity 2020*, Open Technology Institute (last updated July 15, 2020), https://www.newamerica.org/oti/reports/cost-connectivity-2020/focus-on-the-fees/ (in 2020, 123/296 plans had at least a 12-nonth contact term, although some contract lengths were as short as one month and others as long as 24 months). We acknowledge that the Commission has proposed prohibiting video service early termination fees, *see, e.g.*, Press Release, *FCC Takes Action Against Video Service Junk Fees to Protect Consumers and Promote Competition* (Dec. 13, 2023), https://docs.fcc.gov/public/attachments/DOC-398618A1.pdf, but there is no such proposal in place for ISPs, and there likely will not be until the Commission classifies broadband as a Title II service.

[18] 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.

[19] Fed. Trade Comm'n, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* 34 (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"].

purposes other than providing broadband services. Providers log and retain data, like data associated with web browsing or television viewing history, to build and maintain behavioral profiles about consumers for more precise advertising targeting.[20] At least half of the six largest broadband providers the FTC examined (comprising nearly 99% of the mobile internet market)[21] engage in cross-device tracking, which entails correlating data about the same user or household of users across all of their devices.[22] Multiple ISPs have advertising affiliates or their own advertising platforms.[23]

It would be a mistake to rely solely on the FTC's Section 5 authority to regulate privacy practices of internet providers; the Federal Communications Commission must fulfill its statutory role as a privacy regulator. The FTC's 2021 report highlighted a 2017 Memorandum of Understanding between the FTC and FCC as evidence of the two agencies' continued and ongoing coordination and cooperation.[24] It is increasingly important in a connected world that these two agencies be partnered and aligned in the best interests of consumers. The FTC also noted that it has authority to oversee ISPs' internet privacy practices because internet and data services are not a common carrier activity[25] (though to date, the FTC has only publicly brought cases related to malicious ISPs and insecure on-premises equipment such as routers).[26] Classifying broadband as a Title II service would render ISPs common carriers to the extent that

[20] *See id.* at 35.
[21] *See id*. at 3.
[22] *See id*. at 36.
[23] *See id*. at 3, 11-14.
[24] *See id*. at 9 (citing to Restoring Internet Freedom: FCC-FTC Memorandum of Understanding (Dec. 2017), https://www.ftc.gov/policy/cooperation-agreements/restoring-internet-freedom-fcc-ftc-memorandum-understanding). Note also reference to 2015 MOU. *Id*. at 2 ¶ 3; *see also* 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"].
[25] *See id*. at 6.
[26] *See id*. at 7 (citing to *Fed. Trade Comm'n v. Pricewert LLC*, No. C-09-CV-2407 RMW (N.D. Cal. Apr. 8, 2010), https://www.ftc.gov/enforcement/cases-proceedings/092-3148/pricewert-llc-dba-3fnnet-ftc; Letter from Maneesha Mithal, Assoc. Dir. of the Div. of Privacy & Identity Prot., Fed. Trade Comm'n, to Dana Rosenfeld, Partner, Kelley Drye (Nov. 12, 2014), https://www.ftc.gov/system/files/documents/closing_letters/verizon-communications-inc./141112verizonclosingletter.pdf (finding that, while Verizon took steps to mitigate the risk to consumer information, the use of Wired Equivalent Privacy ("WEP") as an encryption standard could leave consumers vulnerable to hackers)).

they act as an ISP[27] (whereas ISP advertising affiliates or platforms would likely not be considered common carriage).

Given the overwhelming evidence of ISPs and other telecommunications service providers engaging in harmful personal data practices—compounded by the lack of comprehensive federal legislation safeguarding consumer privacy and data security—reestablishing the Commission's authority over all telecommunications providers is essential to ensuring Americans' data is protected. As FTC Chair Lina Khan has recently noted, "the Federal Communications Commission has the clearest legal authority and expertise to fully oversee internet service providers."[28] The Commission also has sole jurisdiction of other telecommunications providers to the extent that they are acting as common carriers, putting them beyond the FTC's jurisdiction. We strongly support the application of Title II authority to broadband providers and encourage the Commission to use this authority to ensure that user privacy is protected.

b. Title II's three avenues of protection.

Applying Title II to broadband providers would not only activate all of the protections of 47 U.S.C. § 222 and corresponding regulations, but would also activate the prohibition against unjust and unreasonable practices under 47 U.S.C. § 201(b). This includes the CPNI rules as articulated in 47 U.S.C. § 222(c), 47 U.S.C. § 222(h), and 47 C.F.R. § 64.2010. This also includes the broader carrier privacy obligations articulated in 47 U.S.C. § 222(a) and related Commission enforcement actions.

As EPIC and Public Knowledge noted in the Commission's recent docket on data breach reporting requirements, the Commission has long required carriers to safeguard a wider spectrum of personally identifiable information (PII) and other personal data beyond the explicitly-listed

[27] *See* id. at 5 (citing to *Fed. Trade Comm'n v. AT&T Mobility LLC*, 883 F.3d 848 (9th Cir. 2018), https://www.ftc.gov/enforcement/cases-proceedings/122-3253/att-mobility-llc-mobile-data-service).
[28] Remarks of Chair Lina M. Khan Regarding the 6(b) Study on the Privacy Practices of Six Major Internet Service Providers, Comm'n File No. P195402 (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597790/20211021_isp_privacy_6b_statement_of_chair_khan_final.pdf; Chair Khan went on to say "I support efforts to reassert that authority and once again put in place the nondiscrimination rules, privacy protections, and other basic requirements needed to create a healthier market." Id.

categories in 47 U.S.C. § 222(h).[29] In this section of our comments, we first focus on the Commission's baseline CPNI protections, continue to broader privacy authority under Section 222(a), proceed with the Commission's most general Title II authority under Section 201(b), and conclude by emphasizing the urgent need for regulatory action by the Commission to protect the privacy of telecommunications subscribers.

i. The Commission can apply Title II's CPNI-related protections.

Section 222(c) imposes limitations on carrier disclosure of "customer proprietary network information" (CPNI).[30] The Commission has also promulgated rules related to CPNI use and disclosure under 47 CFR § 64.2001 through 64.2011.[31] Under what is now Section 222(h)(1), Congress has defined CPNI to mean:

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
>
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.[32]

We note that information need only "relate[] to" the enumerated aspects of a user's telecommunications service to be covered by section 222(h)(1)(A). CPNI is not limited, for example, to the exact location at which a user utilizes a carrier's service, but would also include information that *relates to* that location, assuming such information was made available to the carrier solely by virtue of the relationship between the user and the carrier. We encourage the Commission to make use of Title II authority over broadband and other telecommunications

[29] *See* Reply Comments of EPIC, Center for Democracy and Technology, Privacy Rights Clearinghouse, and Public Knowledge, *In re* Data Breach Reporting Requirements, WC Dkt. No. 22-21 at pp. 5-11 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814.
[30] 47 U.S.C. § 222(c).
[31] 47 C.F.R. Part 64, Subpart U, available at https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-U?toc=1; 47 C.F.R. 64.2010 (addressing disclosure specifically).
[32] Originally Section 222(h)(1) was labelled as Section 222(f)(1). *See* Telecommunications Act of 1996, PL 104-104 (Feb. 8, 1996). Section 222(f)(1) was re-assigned to Section 222(h)(1) and "location" was added to the list of CPNI in 1999. *See* Wireless Communications and Public Safety Act of 1999, PL 106-81 (Oct. 26, 1999).

providers to ensure they do not misuse their access to CPNI—for example, by selling SSID-related information which can serve as proxies for location.[33]

ii. The Commission can impose broader carrier privacy and data security obligations under Section 222(a).

Section 222(a) imposes upon every telecommunications carrier the duty "to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers."[34] Note this is "proprietary information" and not the narrower category "customer proprietary network information." The Commission explicitly noted in August 2022 that "[t]he scope of "proprietary information" covered by section 222 extends beyond CPNI data to include private or sensitive data that a customer would normally wish to protect."[35] This includes (but is not limited to) data which would risk physical, emotional, or reputational harm if exposed.[36] In March 2022, the Commission cited to a 2014 case against TerraCom and YourTel for the understanding that 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."[37] The Commission reiterated that all communications service providers "[have] a statutory responsibility to ensure the protection of customer information, including PII and CPNI."[38] Thus, Section 222(a) imposes privacy and data security obligations on Title II-covered entities in addition to the Commission's CPNI-related authorities. For example, the

[33] *See, e.g.*, Stacey Gray, *A Closer Look at Location Data: Privacy and Pandemics*, Future of Privacy Forum (March 25, 2020), https://fpf.org/blog/a-closer-look-at-location-data-privacy-and-pandemics/.
[34] 47 U.S.C. § 222(a).
[35] *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).
[36] *See* FCC Data Breach Reporting Fact Sheet at ¶ 59 ("We find that "harm" to customers could include, but is not limited to: financial harm, physical harm, identity theft, theft of services, potential for blackmail or spam, the disclosure of private facts, reputational or dignitary harm, mental pain and emotional distress, the disclosure of contact information for victims of abuse, and other similar types of dangers. We find that this broader conception of harm is consistent with previous Commission precedent, and we disagree with commenters arguing that "harm" should only include the risk of identity theft or financial harm.") (internal citations omitted).
[37] *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) [hereinafter "2014 NALs"]).
[38] *Id.* at *37 ¶ 82; see also FCC Data Breach Reporting Fact Sheet at ¶ 69 (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)).

Commission recently proposed that its breach notification rules apply to non-CPNI such as Social Security Numbers (SSNs) under this authority.[39] We encourage the Commission to make use of Title II authority over broadband and other telecommunications providers to ensure they safeguard customer proprietary information that may fall outside the typical definition of CPNI, such as SSNs or data that would risk emotional harm if exposed.

iii. The Commission can regulate privacy and data security-related misconduct as unjust or unreasonable practices under Section 201(b).

Section 201(b) of the Communications Act states that: "all charges, practices, classifications, and regulations for and in connection with such communication service, shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful."[40] This is a broad authority that allows the Commission, where Title II applies, to promulgate rules or bring enforcement actions where a common carrier's practices are unjust or unreasonable, including with respect to their privacy and data security practices. In addition to 222(a) violations, in the Commission's 2014 enforcement action against TerraCom and YourTel, the agency pointed to carrier violations of Section 201(b).[41] These Section 201(b) violations included: failing to protect and secure the proprietary information of their customers,[42] making representations to customers in their privacy policies that were false, deceptive, and misleading,[43] and notifying anything less than all potentially affected consumers of the breach.[44] The Commission explicitly stated that "carriers are now on notice that in the future we fully intend to assess forfeitures for such violations."[45] Problems of inadequate notification still persist today,[46] likely in the context of ISPs as well. The Commission

[39] See, e.g., FCC Data Breach Reporting Fact Sheet at ¶¶ 15-17; *see also* Press Release, FCC Adopts Updated Data Breach Notification Rules to Protect Consumers (Dec. 13, 2023), https://www.fcc.gov/document/fcc-adopts-updated-data-breach-notification-rules-protect-consumers.
[40] 47 U.S.C. § 201(b).
[41] *See* 2014 NALs, available at: https://docs.fcc.gov/public/attachments/FCC-14-173A1_Rcd.pdf.
[42] *See id*. at ¶ 31.
[43] *See id*. at ¶ 38.
[44] *See id*. at ¶ 39.
[45] *Id*. at ¶ 43, n 97.
[46] *See, e.g.*, Lorenzo Franceschi-Bicchierai, *23andMe confirms hackers stole ancestry data on 6.9 million users*, TechCrunch (Dec. 4, 2023), https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/; Lily Hay Newman, *Okta Breach Impacted All Customer Support Users—Not 1 Percent* (Nov. 29, 2023), https://www.wired.com/story/okta-breach-disclosure-all-customer-support-users/; Press Release, FTC Takes Action Against Global Tel*Link Corp. for Failing to

drew upon its 201(b) authority again in 2015, in both privacy and data security contexts.[47] Commissioner Starks has emphasized privacy and data security in the context of Commission matters grounded in the Commission's 201(b) authority.[48]

We encourage the Commission to make use of Title II authority over broadband and other telecommunications providers to ensure they do not fail to protect proprietary information, do not make false or misleading representations in privacy policies, do notify all impacted consumers when a breach occurs,[49] and take other actions as necessary to protect consumers and the public interest.

The Commission's authority under 201(b) is analogous to the FTC's section 5 powers. Section 5 of the FTC Act prohibits unfair or deceptive acts or practices,[50] including harmful data practices.[51] Section 201(b) of the Communications Act prohibits "any charge, practices,

---

Adequately Secure Data, Notify Consumers After Their Personal Data Was Breached (Nov. 16, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-takes-action-against-global-tellink-corp-failing-adequately-secure-data-notify-consumers-after; Press Release, AG Henry Announces $49.5 Million Settlement with Blackbaud for Data Breach That Impacted Millions of U.S. Consumers (Oct. 5, 2023), https://www.attorneygeneral.gov/taking-action/ag-henry-announces-49-5-million-multistate-settlement-with-blackbaud-for-data-breach-that-impacted-millions-of-u-s-consumers/.

[47] *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.)").

[48] *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.").

[49] *See, e.g.*, FCC Data Breach Reporting Fact Sheet at ¶ 29.

[50] *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).

[51] 47 U.S.C. § 201(b).

classification, or regulation that is unjust or unreasonable."[52] 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 Title II-covered carriers. Both agencies have documented this understanding of their analogous authorities in a 2015 Consumer Protection Memorandum of Understanding (CP MOU) between the Commission and the FTC, which articulates that the agencies "will continue to work together to protect consumers from acts and practices that are deceptive, unfair, unjust and/or unreasonable."[53] 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."[54] This is largely consistent with the 2017 MOU between the agencies, which explicitly notes that "nothing in this [2017] Memorandum should be construed as altering, amending, or invalidating [the 2015 CP MOU and a 2003 telemarketing MOU]."[55] The agencies clearly (and correctly) contemplate parallel authority between Section 5 and Section 201(b). There have been many attempts by industry players to frame the FTC and FCC privacy authorities as either competing or inconsistent, but nothing is further from the truth. These agencies can and should work together to defend the privacy of internet users. Indeed, the best interests of consumers will be served by the FTC and FCC working in parallel to ensure that harmful privacy practices are prevented across all industries through a combination of rulemaking, regulatory guidance, and enforcement.

[52] CP MOU.
[53] *Id*. at 2.
[54] 2014 NALs at ¶ 53. The Commission also noted that "[h]ad Congress wanted to limit the protections of subsection [222](a) to CPNI, it could have done so," id. at ¶ 15. *See also In re* Advanced Methods to Target and Eliminate Unlawful Robocalls, Fourth Report and Order, CG Docket No. 17-59 at ¶ 37 (Dec. 30, 2020) ("Section 201(b) and 202(a) grant us broad authority to adopt rules governing just and reasonable practices of common carriers").
[55] *See* Restoring Internet Freedom: FCC-FTC Memorandum of Understanding (Dec. 2017), https://www.ftc.gov/policy/cooperation-agreements/restoring-internet-freedom-fcc-ftc-memorandum-understanding.

iv. The Commission must invoke its Title II authority now.

As we articulated in subsection II(a), timely protections are essential to safeguard consumers and their families from the malicious and negligent practices of broadband and other telecommunications service providers. As we outlined in the subsections II(b)(i), (ii), and (iii), application of the Commission's Title II authority to ISPs would unlock CPNI protections, activate privacy obligations for non-CPNI personal data such as PII and proprietary information, and enable the Commission to take broadband providers to task for unjust or unreasonable data security and privacy practices. This could allow for the Commission to enact data minimization and purpose specification rules for consumer data, comporting with the Fair Information Practices first endorsed by the federal government in 1973[56] and applied by numerous federal, state, and international regulators over the last 50 years. The Commission's MOU with the FTC would allow the two agencies to work cooperatively, and would entrust the Federal Communications Commission to protect the privacy and security of consumer data to the extent that the broadband provider is acting in their capacity as a common carrier. As the Commission itself notes, even beyond privacy and data security protections for consumers, there are also positive implications for national security and for bundled services in applying Title II to broadband service providers.[57]

III. The Commission's application of Title II authority would help combat consent fraud and brokering.

The Commission asks whether Title II classification of broadband would enhance the Commission's authority to support consumer privacy by combatting illegal robocalls and robotexts.[58] Scams remain a pervasive problem, as the latest consumer loss data from the FTC indicates[59] (data which does not even reflect the additional nuisance cost of other unwanted and illegal calls and texts, such as telemarketing calls). Title II authority would enhance the Commission's ability to combat consent fraud and brokering.

---

[56] *See* Fair Information Practice Principles (FIPPs), Federal Privacy Council, https://www.fpc.gov/resources/fipps/ (last visited Dec. 13, 2023).
[57] *See* NPRM at ¶ 42-44.
[58] *See* NPRM at ¶ 45.
[59] *See, e.g.*, FTC Consumer Sentinel Network, Fraud Reports by Contact Method, Reports & Amount Lost by Contact Method, available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts.

It is our understanding that unwanted calls and texts are often the result of contact information and other personal information being exchanged amongst data brokers.[60] While we expect that the Commission's imminent Second Report and Order in dockets 21-402, 02-278, and 17-59 will address the issue of TCPA consent brokering,[61] the Commission is right to note in the instant NPRM that "bad actors continue to evolve their techniques to find new ways to interrupt consumers and perpetuate fraud."[62] Title II authority will better position the agency to take action against these emerging tactics.

IV. The Commission should explicitly state that it does not preempt state privacy and consumer protection laws.

In the interest of clarity, the Commission should explicitly state that it is not preempting state privacy and consumer protection laws in classifying broadband providers as telecommunications services governed by Title II.[63] Congress has not directed the Commission to preempt states on privacy in Section 222 or elsewhere in Title II.[64] Indeed, there are multiple examples of state regulators that have brought privacy-related enforcement actions against phone companies that have historically been regulated by the Commission under Title II.[65]

---

[60] *See, e.g.*, FTC ISP Report at 27.

[61] *See* Press Release, FCC Adopts New Rules to Close the 'Lead Generator' Robocall and Robotexts Loophole and Facilitate Blocking of Unwanted Robotexts (Dec. 13, 2023), https://www.fcc.gov/document/fcc-closes-lead-generator-robocall-loophole-adopts-robotexts-rules; *see also* FCC Fact Sheet, Combatting Illegal Text Messages, CG Dkt. Nos. 02-278, 21-402, 17-59 (Rel. Nov. 22, 2023), https://docs.fcc.gov/public/attachments/DOC-398661A1.pdf.

[62] NPRM at ¶ 45.

[63] *See* NPRM at ¶ 96.

[64] *See, e.g.*, Congressional Research Service, *ACA Connects v. Bonta*: Ninth Circuit Upholds California's Net Neutrality Law in Preemption Challenge (Feb. 2, 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10693. This is to be distinguished from state regulation of provision of services which Congress explicitly gave the FCC preemption authority over in Section 253 of Title II. *See, e.g.*, Congressional Research Service, Stepping In: The FCC's Authority to Preempt State Laws Under the Communications Act at 9, 23-31 (updated Sept. 20, 2021), https://crsreports.congress.gov/product/pdf/R/R46736.

[65] *See, e.g.*, Reuters, *Massachusetts is probing huge T-Mobile data breach* (Sept. 14, 2021), https://www.reuters.com/legal/litigation/massachusetts-is-probing-huge-t-mobile-data-breach-2021-09-14/ (referring to Aug. 2021 breach, noting that the Commission even opened its own investigation, citing to Reuters, *U.S. telecoms agency to probe T-Mobile data breach* (Aug. 18, 2021), https://www.reuters.com/technology/hackers-steal-some-personal-data-about-78-mln-t-mobile-customers-2021-08-18/); Press Release, AG Healey Secures $16 Million From Multistate Settlements With Experian and T-Mobile Over Data Breaches (Nov. 17, 2022), https://www.mass.gov/news/ag-healey-secures-16-million-from-multistate-settlements-with-experian-and-t-mobile-over-data-breaches (referring to 2015 breach); Todd Bishop, *Washington state AG says T-Mobile wrongfully withholding documents in security*

Additionally, the Commission recently announced an enforcement partnership between its Privacy and Data Security Task Force and multiple State Attorneys General, explicitly noting that it expects state and federal agencies to take coordinated enforcement action under sections 201 and 222 of the Communications Act.[66] Just as these state actions and partnerships were not preempted by Title II, Title II classification should not immunize broadband and other telecommunications providers from privacy and data security enforcement actions under state law. Given that states are often leaders in digital privacy and data security,[67] and given that preemption would put additional burdens on the Commission's resources as the primary enforcement authority, the Commission should not seek to preempt state privacy and consumer protection laws. Indeed, the Commission should explicitly clarify that its Title II authority does not preempt these state laws. Courts have already recognized the need for states to act in the absence of federal regulation,[68] and it would be consistent with the Commission's mandate under Title II for states to be able to impose stricter privacy rules on common carriers.

V. The Commission should immediately initiate a consumer privacy and data security rulemaking under Title II.

An additional benefit to consumers of applying Title II to broadband services is the ability of the Commission to advance a privacy and data security rulemaking. Although the 2017 joint disapproval of the Commission's 2016 Privacy Order under the Congressional Review Act does not directly implicate the Commission's Title II classification, we urge the Commission to undertake reclassification with an eye towards a renewed privacy rule. In 2023, this rulemaking and the rulemaking on data breach reporting requirements could be the first major consumer privacy rules with staying power that the Commission has enacted in more than 15 years; the agency needs to continue with accelerated measures to meet the threats presented to Americans' data and to trust in our country's communications infrastructure.

probe, GeekWire (June 15, 2023), https://www.geekwire.com/2023/washington-state-ag-accuses-t-mobile-of-wrongly-withholding-documents-in-security-probe/ (referring to August 2021 breach).

[66] *See* Press Release, FCC Privacy & Data Protection Task Force Launches First-Ever Enforcement Partnership with State Attorneys General (Dec. 6, 2023), https://docs.fcc.gov/public/attachments/DOC-398939A1.pdf.

[67] *See, e.g.*, California Consumer Privacy Act Regulations, California Privacy Protection Agency, https://cppa.ca.gov/regulations/consumer_privacy_act.html (last visited Dec. 13, 2023).

[68] *See ACA Connects v. Bonta*, 24 F. 4th 1233, 1237 (9th Cir. 2022).

The Commission should act quickly to promulgate new Title II privacy rules that will bring broadband and other telecommunications providers into compliance with the data minimization requirements and other timely privacy standards being established at the federal and state level. Privacy regulation has moved far beyond the failed notice-and-choice approach of the 1990s.[69] Strong data minimization standards require limiting the collection, use, transfer, and retention of personal information to that which is reasonably (or in some cases strictly) necessary.[70] Although data minimization has been enshrined as a Fair Information Practice since the 1973 HEW Report,[71] it has gained renewed attention as privacy policies have proven utterly ineffective at empowering consumers and protecting their personal data from misuse.[72] Commissioner Starks has pushed for data minimization to be an important part of innovation in the broadcast industry.[73] The FTC has brought numerous enforcement actions that require limited data collection as part of the consent decree;[74] some such actions additionally restrict use through purpose limitations.[75] The CFPB has also proposed collection, use, and retention limitations in a recent data rights rulemaking.[76] Especially given ISPs' unexpected secondary use

[69] *See, e.g.*, Sara Geoghegan, *Data Minimization: Regulating the Ineffective, Irrelevant, and Invasive Practice of Surveillance Advertising* (Aug. 8, 2023), https://epic.org/data-minimization-regulating-the-ineffective-irrelevant-and-invasive-practice-of-surveillance-advertising/.
[70] *See* id.
[71] *See* U.S. Dept. of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (July 1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.
[72] *See, e.g.*, Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A Journal of Law and Policy for the Information Society no. 3, 543-568 (Winter 2008/2009), available at https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.
[73] *See* Speech, Starks Remarks on the Future of Broadcast Television 6 (Oct. 18, 2022), https://www.fcc.gov/document/starks-remarks-future-broadcast-television ("How can they follow the important principle of data minimization, and work to achieve their goals with a minimum of data collected, stored, and shared?").
[74] *See, e.g.*, Fed. Trade Comm'n, Decision and Order, *In re* Global Tel*Link Corp., et al., File No. 2123012 at 11 ¶ E(12) (Nov. 16, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2123012-global-tel-link-corporation; Fed. Trade Comm'n, Decision and Order, *In re* Chegg, Inc., File No. 2023151 at 6 ¶ E(4); *see also* Complaint, *In re* Chegg, Inc., FTC File No. 2023151 at ¶ 9(f) (Oct. 31, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf.
[75] *See, e.g.*, Fed. Trade Comm'n, Consent Order, *In re* Drizly, LLC, et al., File No. 2023185 at 14-15, https://www.ftc.gov/system/files/ftc_gov/pdf/2023185-drizly-combined-consent.pdf (Sections II and III).
[76] *See, e.g.*, Consumer Financial Protection Bureau, Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights 40-45 (Oct. 27, 2022), https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf (Section E.1. Limiting the collection, use, and retention of consumer-authorized Information). In the context of financial data especially, Brookings has reported overwhelming

of consumer data as outlined in the FTC staff report, the Commission should consider how data minimization—including purpose and retention limitations—could better protect Americans.

Title II authority could advance other consumer data protection goals as well. It would enable the Commission to require fundamental minimum cybersecurity practices that evolve over time,[77] not merely a generic "reasonableness" standard with no floor. The Commission could support the FTC in protecting consumers from the harms of AI models such as discriminatory targeted advertising practices that are built from online activity data. The Commission could also utilize its license revocation authority where Title II applies.[78] We encourage the Commission to consider the full scope of what is necessary to advance the public interest and how it can achieve this with Title II authority.

To that point, the Commission asks about the adequacy of consumer relief for ISP-perpetrated harms in the wake of the Restoring Internet Freedom (RIF) Order.[79] Reforms are certainly needed here in order to adequately protect consumers. We believe that the Supreme Court's regrettable 2021 ruling restricting the FTC's ability to seek monetary relief on behalf of consumers reduces the deterrent effect of FTC enforcement actions.[80] And we agree with the Commission that the RIF Order's assumption that ISP-perpetrated consumer harms would be

---

support for data minimization and purpose limitations, across multiple demographics. *See, e.g.*, Dan Murphy and Jennifer Tescher, *Policymakers must enable consumer data rights and protections in financial services* (Oct. 20, 2021), https://www.brookings.edu/articles/policymakers-must-enable-consumer-data-rights-and-protections-in-financial-services/.

[77] *See, e.g.*, Report and Order and Further Notice of Proposed Rulemaking, *In re* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, IP-Enabled Services, CC Dkt. No. 96-155, WC Dkt. No. 04-36 at ¶ 15 (Rel. Apr. 2, 2007), https://docs.fcc.gov/public/attachments/FCC-07-22A1.pdf (expecting that flexibility given to carriers in password protection practices will enable them to design authentication programs that continue to evolve to fight pretexter efforts); id. at ¶ 67 (noting the Commission's own duty to ensure that the consumer protection objectives of the Communications Act are maintained as technologies evolve).

[78] *See* NPRM at ¶ 27.

[79] *See, e.g.*, NPRM at ¶ 140-43.

[80] *See* NPRM at ¶ 139 (citing to Press Release, FTC Asks Congress to Pass Legislation Reviving the Agency's Authority to Return Money to Consumers Harmed by Law Violations and Keep Illegal Conduct from Reoccurring, Federal Trade Commission (Apr. 27, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/04/ftc-asks-congress-pass-legislation-reviving-agencys-authority-return-money-consumers-harmed-law (discussing an "April 22 ruling by the U.S. Supreme Court that eliminated the FTC's longstanding authority under Section 13(b) of the FTC Act to recover money for harmed consumers").).

obvious and widespread is belied by the recent FTC staff report; indeed, these harmful practices can be opaque even to regulators let alone to consumers.[81]

VI. The Commission should update the transparency rule.

The Commission asks about enhancing disclosures required by the transparency rule.[82] As EPIC argued in the docket on the Commission's proposed broadband nutrition labels, we believe three simple questions would immensely improve a consumer's ability to understand how their data is being collected and used by their ISPs: (1) is personal information collected for purposes other than providing broadband service (hereinafter "other purposes"); (2) is personal information shared with third parties for other purposes; and (3) can the consumer opt out of the collection, use, or sharing of personal information for other purposes (with a link to the opt-out method if the answer is yes).[83] We also believe it would be valuable to include cybersecurity information on a secondary layer of the label, as EPIC and Public Knowledge argued in the Commission's docket on labels for Internet of Things devices.[84] However, we will elaborate on those points in that proceeding (PS 23-239) and in the broadband nutrition label proceeding (CG 22-2) rather than here.

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 broadband and other telecommunications providers accordingly.

[81] *See, e.g.*, FTC ISP Report at 17, 26 n 100, 31, 36.
[82] *See* NPRM at ¶ 173-76.
[83] *See* Comments of EPIC, *In* re Empowering Broadband Consumers through Transparency, CG Dkt. No. 22-2 (Mar. 9, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/10310177612037; *see also* Comments of Center for Democracy and Technology, EPIC, and Ranking Digital Rights, *In* re Empowering Broadband Consumers through Transparency, CG Dkt. No. 22-2 (Feb. 16, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/102161424008021.
[84] *See* Reply Comments of EPIC, Clinic to End Tech Abuse, Madison Tech Clinic, Public Knowledge, and Ranking Digital Rights, *In* re Cybersecurity Labeling for Internet of Things, PS Dkt. No. 23-239 (Nov. 10, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/111054758013.

Respectfully submitted, December 14, 2023.

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