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

| | |
|---|---|
| Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information | CC Dkt. No. 95-115 |

**COMMENTS OF**
**ACCESS NOW, CENTER FOR DIGITAL DEMOCRACY, CONSUMER ACTION, CONSUMER FEDERATION OF AMERICA, CONSUMER REPORTS, ELECTRONIC PRIVACY INFORMATION CENTER, FREE PRESS, MEDIA ALLIANCE, NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE, PRIVACY RIGHTS CLEARINGHOUSE, PUBLIC KNOWLEDGE, AND STOP ONLINE VIOLENCE AGAINST WOMEN**

Access Now, Center for Digital Democracy, Consumer Action, Consumer Federation of America, Consumer Reports, Electronic Privacy Information Center, Free Press, Media Alliance, New America's Open Technology Institute, Privacy Rights Clearinghouse, Public Knowledge, and Stop Online Violence Against Women (collectively, "Commenters") submit these joint comments in response to the above-referenced docket.[1] Commenters are all nonprofit organizations focused on protecting privacy rights that are at risk of abuse. Due to the important and sensitive information contained within Consumer Proprietary Network Information (CPNI), Commenters urge the FCC to uphold and improve privacy protections for CPNI. Under no circumstances should the FCC eliminate or otherwise weaken any of the valuable protections currently applicable to CPNI.

The Federal Communications Commission (FCC) should keep the CPNI certification regulations to protect consumers from violations of their privacy by carriers. The certification

[1] Information Collection Being Reviewed by the Federal Communications Commission, *Notice and Request for Comments*, 85 Fed. Reg. 50,824 (Aug. 18, 2020).

rules in question require an officer or agent of a carrier to annually certify that their company has adopted adequate CPNI protection procedures and explain how they function.[2] The certificate must also include an explanation of actions taken against data brokers along with a summary of all customer complaints concerning the carrier's unauthorized release of CPNI.[3] Removing these certification requirements would hinder the FCC's ability to deter the misuse of CPNI while failing to relieve carriers of significant compliance burdens. In evaluating the burdens imposed by CPNI certification requirements, the FCC should consider all the benefits this rule confers alongside the harm it prevents. The FCC's responsibility as a regulator of CPNI is far from overreaching—and is more crucial than ever in this interconnected age.

Furthermore, curtailing CPNI protections would be inappropriate at this time due to the unique conditions brought on by the current Covid-19 pandemic. Due to social distancing guidelines, consumers are more reliant than ever on telecommunication technology that could be rendered unsafe by the reduction of privacy protections.[4] With no clear end to the pandemic in sight, now is not the time to be reconsidering CPNI requirements.

## I. CPNI MUST REMAIN PROTECTED

CPNI represents a cornerstone of the larger data privacy landscape that must contend with increasingly grave threats from misuse by state and private actors.[5] When collected by

---

[2] 47 C.F.R. §64.2009(e).

[3] *Id*.

[4] *See* Katherine Guyot and Isabel V. Sawhill, *Telecommuting Will Likely Continue Long After the Pandemic*, Brookings Institute (Apr. 6, 2020), https://www.brookings.edu/blog/up-front/2020/04/06/telecommuting-will-likely-continue-long-after-the-pandemic/; Compliance Filing of Zoom Voice Communications, Inc., *CPNI Compliance Statement of Operating Procedures – 2019 Reporting Period*, Dkt. 06-36 (filed Jul. 31, 2020).

[5] *E.g.*, Press Release, FED. TRADE COMM'N, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (Jul. 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related; *Sprint Confirms Data Breach for Second Time in 2019*, Security Mag. (Jul. 18, 2019), https://www.securitymagazine.com/articles/90560-sprint-confirms-data-breach-for-second-time-in-2019.

carriers, CPNI has a number of applications that justify heightened protections because its misuse can negatively impact the most intimate rights to privacy and autonomy that individuals possess. Call metadata, for example, gives carriers access to information on the length, general location, and phone numbers involved in a call that can be aggregated to reveal everything from sleeping habits to personal relationships.[6] As computer scientist Ed Felten—now a member of the Privacy and Civil Liberties Oversight Board—stated before the Senate Judiciary Committee in 2013,

> Metadata can expose an extraordinary amount about our habits and activities. Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social attitudes; the number of friends we have; and even our civil and political affiliations.[7]

Another computer scientist, Vitaly Shmatikov, explained to the FCC in 2014 that location-related CPNI can reveal "the route of the person's highway commute and the path taken when walking his or her children to school."[8]

Moreover, telecommunications metadata is becoming more, not less, sensitive and deserving of close protection. As the FCC itself explained just this year in Notices of Apparent Liability against the four major wireless carriers for CPNI misuse:

> The wireless phone is a universal fixture of modern American life. Ninety-six percent of all adults in the United States own a mobile phone. . . .

---

[6] *See* Public Knowledge, et al. Comments Letter on Big Data and Consumer Privacy in the Internet Economy, Dkt. 4424–01, at 2-3 (filed Aug. 5, 2014).

[7] Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing before the S. Comm. on the Judiciary, 113th Cong. 8-10 (2013) (statement of Edward Felten, Professor of Computer Science and Public Affairs, Princeton University) available at https://www.judiciary.senate.gov/imo/media/doc/10-2-13FeltenTestimony.pdf.

[8] Comments of Vitaly Shmatikov to the Public Knowledge Petition for Declaratory Ruling, WC Docket No. 13-306 at 2-3 (March 2, 2014), available at https://ecfsapi.fcc.gov/file/7521087284.pdf.

> More than almost any other product, consumers "often treat [their phones] like body appendages." The wireless phone goes wherever its owner goes, at all times of the day or night. For most consumers, the phone is always on and always within reach. And every phone must constantly share its (and its owner's) location with its wireless carrier because wherever it goes, the networks must be able to find it to know where to route calls.[9]

Furthermore, the public has expressed concerns regarding data privacy that the FCC can help address by upholding CPNI certification requirements. Apprehension toward the lack, not excess, of adequate privacy protections is well documented.[10] In 2019, the Pew Research Center conducted a nationwide poll that found over eighty percent of Americans felt they had little to no control over how corporations or the government used their data.[11] Seventy-five percent of respondents were in favor of *more*, not *less*, government regulation over companies with access to their personal information.[12] A more recent June 2020 survey echoes the findings from the Pew polls, with over ninety percent of respondents preferring to do business with companies that prioritize their data privacy.[13] Consumers are eager for the FCC to stand up for their right to privacy by taking more steps to protect sensitive CPNI, not less.

---

[9] *Sprint Corp.*, 35 FCCR 1655, ¶1 (2020); *Verizon Communications,* 35 FCCR 1698, ¶1 (2020); *AT&T Inc.*, 35 FCCR 1743, ¶1 (2020); *T-Mobile USA, Inc.*, 35 FCCR 1785, ¶1 (2020).

[10] *See* Brooke Auxier and Lee Rainie, *Key takeaways on Americans' views about privacy, surveillance and data-sharing*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/, *see also Brooke* Auxier et. al, *Americans, and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019) (provides the primary source for which the conclusions in the first article are drawn), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[11] Auxier, *Key Takeaways*, Pew Research Center (2019).

[12] *Id*.

[13] *Id;* Kyle Daly, *Exclusive: Poll reveals Americans' data privacy frustrations*, Axios (Aug. 13, 2020), https://www.axios.com/exclusive-poll-reveals-americans-data-privacy-frustrations-16514f76-ff5e-4df1-929e-6ba259268023.html.

Meeting these privacy needs hinges on cooperation between the FCC and its constituencies. Entertaining dismantling long-held CPNI certification requirements in the face of growing public concerns about privacy is not an appropriate regulatory action at this time. Growing tension between the public's desire for more government action and the decline in administrative activity presents an opportunity for the FCC to reassert its position as the defender of CPNI privacy.

## II. CERTIFICATIONS ARE KEY TO PROTECTING CPNI PRIVACY

Because the FCC has given carriers considerable flexibility "in determining how they will ensure their compliance with CPNI rules,"[14] certifications ensure compliance with each carrier's individualized privacy safeguards. Carriers need not follow a one-size-fits-all approach in protecting privacy because some do not have physical stores and corresponding in-person verification for access to CPNI or use CPNI for marketing purposes. Alternatively, there are certain reasonable safeguards that every carrier must be bound to, like personnel training, but how each carrier complies may vary. Regardless of the wide variety of compliance procedures carriers have adopted, an officer's certification confirms their company has taken the necessary steps to protect CPNI.[15] It is easier for an officer to ensure compliance with CPNI safeguards than, say, the FCC to ensure compliance through investigations of each carrier. The FCC decided at least one officer must have personal knowledge of compliance procedures to keep companies honest and protect CPNI privacy.[16]

---

[14] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 14 FCCR 14409, ¶127 (1999) ("*CPNI Reconsideration*").

[15] *See* 47 CFR 64.2009(e).

[16] *See CPNI Reconsideration*, 14 FCCR 14409, ¶127.

When officers have personal knowledge of compliance procedures but CPNI is still being exploited, the FCC can and should hold officers liable for their false certifications.[17] Forfeitures by carriers are not enough to ensure compliance on their own, as evidenced by the fact that carriers persist in misusing CPNI.[18] Holding officers liable would motivate them to ensure carriers are following the law. Carriers have been liable for forfeitures in the past due to non-filing of certifications.[19] But certifications are a valuable tool for accountability. By requiring carriers to attest that they are meeting their obligations to protect CPNI, the certification requirement obliges them to review the procedures they have in place to ensure that they can account for the proper treatment of customers' data.

The circumstances leading to the FCC's March 2020 enforcement action demonstrated that the threats facing CPNI are dire.[20] The wanton sale of CPNI access by carriers, coupled with their continuous refusal to stop this activity even after being exposed,[21] revealed just how brazen some carriers have become.[22] With the general decline in FCC action, it appears as though carriers are shirking their responsibility to consumers.[23] Despite the most recent bad behavior from carriers, the FCC is more than capable of catching wrongdoers and using regulations like

[17] 18 USC § 1001.

[18] *See infra* notes 17–21 and accompanying text.

[19] *See Annual CPNI Certification, Omnibus Notice of Apparent Liability for Forfeiture*, 25 FCCR 1790 (2010) (Combined agency action that would only impose fines on 7 companies for failing to file CPNI certification statements in 2008, of which 5 were ultimately upheld); *Annual CPNI Certification, Omnibus Notice of Apparent Liability for Forfeiture and Order*, 26 FCCR 2160 (2011) (Combined agency action that would impose fines on 10 companies for failing to file CPNI certification statements between 2009 and 2010, of which 7 were ultimately upheld).

[20] AT&T Inc., 35 FCCR 1743 (2020).

[21] *Id*.

[22] *E.g., AT&T Inc.*, 35 FCCR 1743, ¶3 (2020) (explaining that "even after highly publicized incidents put [AT&T] on notice that its safeguards for protecting customer location information were inadequate, AT&T apparently continued to sell access to its customers' location information for nearly a year.").

[23] *See Id.*

the certification requirements to induce compliance.[24] The revival of CPNI enforcement could be a useful way to discipline carriers if the FCC pursues violators more actively.

Moreover, the FCC certification requirements were adopted in 1998, and since then other agencies have passed similar requirements that showcase their efficacy. After adopting certification rules in the early 2000s, the Securities and Exchange Commission has pursued causes of action against officers for false certifications of financial reports.[25] The Department of Commerce, which is the administrator of the EU/US Privacy Shield established in 2016, requires a yearly certification signed by a corporate officer with misrepresentations possibly actionable under 18 U.S.C. § 1001.[26] Though the European Court of Justice declared invalid the EU Commission's decision on the adequacy of the EU-U.S. Privacy Shield, the Federal Trade Commission (FTC) expects companies to continue to comply with their obligations.[27] Furthermore, in 2019, the FTC began to require annual certifications of compliance from officers to meet the terms of its data security orders.[28] The most prominent example was the FTC's recent modified order regarding Facebook, which was revealed in 2019 to have broken the privacy promises it made to the FTC in 2012.[29] The FTC's justification for certification requirements is partly based on studies that suggest "board [of directors] attention to data security decisions can

---

[24] *Id*.
[25] 17 C.F.R. § 240.13a–14; *See, e.g., U.S. Sec. & Exch. Comm'n v. Jensen,* 835 F.3d 1100, 1111-1112 (9th Cir. 2016).
[26] *Self-Certification*, DEP'T OF COM., https://www.privacyshield.gov/article?id=6-Self-Certification (last visited Sept. 26, 2020).
[27] *Update on the Privacy Shield Framework*, FED. TRADE COMM'N (July 21, 2020), https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield.
[28] *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers*, FED. TRADE COMM'N (Jan. 6, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance.
[29] *See FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

dramatically improve data safeguarding."[30] With the growing adoption of certification requirements to combat serious abuses of consumer trust, it would be anachronous and arbitrary for the FCC to dispose of its existing CPNI certifications now.

## III. CERTIFICATION REQUIREMENTS ARE NOT BURDENSOME ENOUGH TO JUSTIFY THEIR REPEAL

The FCC should not dispose of its certification rules because they are not unreasonably burdensome, especially on balance with their usefulness. Certifications do not entail much more than supervising reasonable and adequate data privacy practices.[31] The bulk of the work that goes into CPNI compliance surely is in ensuring that each department within a carrier is not abusing CPNI, not in simply issuing a periodic certification that that work has been done.

By now, carriers should have well-established processes for gathering the required information for filing certifications, which are usually only a few pages.[32] Most large and small carriers seem to have had no problems recently with filing timely certifications by the deadline, despite earlier complaints about the burden of including a summary of customer CPNI complaints and actions taken against data brokers.[33]

Large carriers have adequate resources for compliance with these certifications. Indeed, many large carriers had few customer CPNI complaints and actions taken against data brokers in 2019.[34] But outliers like AT&T and T-Mobile received over 500 and 1000 complaints,

---

[30] *Id*.

[31] *See* 47 CFR 64.2009(e).

[32] *See e.g.*, Compliance Filing of Atlantech Online Inc., *CPNI Compliance Certification Annual Filing*, Dkt. 06-36 (filed Feb. 11, 2019). (four-page long small carrier filing).

[33] *E.g.*, Reply Comments of MetroPCS Communications Inc., *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Dkt. 96-115, at 18 (filed June 1, 2006); Reply Comments of T-Mobile USA, Inc., *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Dkt. 96-115, at 6 (filed June 1, 2006).

[34] *E.g.*, Compliance Filing of Charter Communications Inc., *CPNI Compliance Certification Annual Filing*, Dkt. 06-36 (filed Feb. 27, 2020); Compliance Filing of Sprint Corp., *CPNI Compliance Certification Annual Filing*, Dkt. 06-

respectively.[35] A deficient carrier brings such a large discrepancy in complaints, and concomitant filing requirements, on itself. Looking for such discrepancies in complaint volume across carriers can help the FCC identify the worst offenders for enforcement action.

Small carriers do not appear to be particularly burdened by the certification requirements either. Small carriers rarely have either customer complaints or actions against data brokers to report.[36] This is likely because they have a closer connection to their relatively few customers and thus are less likely to abuse CPNI in the first place. It is also easier for small carriers to supervise the extent to which they use CPNI since they have fewer employees. And as the FCC has noted, the privacy of small carriers' customers is no less important than that of large carriers' customers.[37] Congress intended "every telecommunications carrier" to safeguard CPNI privacy.[38] Despite this, if the FCC finds that this is an unreasonable burden to small carriers, it could provide "an exemption from coverage of the rule, or any part thereof," as allowed by the Regulatory Flexibility Act.[39] The FCC has made such exemptions in the past, specifically under the now defunct 2016 FCC order extending CPNI-style privacy protections to broadband providers.[40] In its order, the FCC exempted telecommunication carriers that do not deal in broadband services from having to abide by the additional compliance burdens so long as the

36 (filed Mar. 2, 2020); Compliance Filing of Verizon, *CPNI Compliance Certification Annual Filing*, Dkt. 06-36 (filed Feb. 19, 2020).

[35] Compliance Filing of AT&T Services, Inc., *CPNI Compliance Certification Annual Filing*, Dkt. 06-36 (filed Feb. 25, 2020); Compliance Filing of T-Mobile US, Inc., *CPNI Compliance Certification Annual Filing*, Dkt. 06-36 (filed Feb. 25, 2020).

[36] *E.g.*, Compliance Filing of Atlantech Online Inc., *CPNI Compliance Certification Annual Filing*, Dkt. 06-36 (filed Feb. 11, 2019).

[37] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 17 FCCR 14860, 14938, ¶12 (2002); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 13 FCCR 8061, ¶236 (1998).

[38] 47 U.S.C. § 222(a).

[39] 5 U.S.C. § 603(c)(4).

[40] *See In the Matter of Protecting the Privacy of Customers of Broadband & Other Telecommunications Services*, 31 FCCR 13911 (2016).

company "addresses the issues of transparency, choice, data security, and data breach and provides a mechanism for the customer to communicate with the carrier about privacy and data security concerns."[41] A similarly permissive exemption for smaller carriers would be sure to assuage the FCC's concern over the impact of strict compliance burdens on small businesses without posing undue risk to the privacy of CPNI held by larger carriers.[42]

## CONCLUSION

For the foregoing reasons, Commenters urge the FCC to retain the CPNI certification rules as-is. The burden of the certification requirement is not unreasonable considering the importance of CPNI privacy, repeated abuses of consumers' sensitive information despite other safeguards and the imposition of forfeitures, the certifications' potential usefulness in enforcement, and their growing adoption by other agencies. Therefore, the FCC should retain the CPNI certification rules unchanged.

/s/

Laura M. Moy
Institute for Public Representation[43]
Georgetown University Law Center
600 New Jersey Avenue NW
Washington, DC 20001
Tel. (202) 662-9535
Laura.Moy@georgetown.edu
*Counsel for Commenters*

*Filed October 19, 2020*

[41] *Id*.

[42] *See Protecting & Promoting the Open Internet*, Dkt. No. 14-28, Notice of Proposed Rulemaking, 29 FCCR 5561, 5615-16 (2014)

[43] These comments were drafted with considerable assistance by Tyler Kaufman and Nicholas Paniagua, students in the Communications & Technology Law Clinic of the Institute for Public Representation, and Victoria Tang, a teaching fellow in the same clinic.