University of St. Thomas Journal of Law and Public Policy

Volume 11 | Issue 1 Article 3

Broadband Privacy within Network Neutrality: The FCC's Application & Expansion of the CPNI Rules

Justin S. Brown

BROADBAND PRIVACY WITHIN NETWORK NEUTRALITY: THE FCC'S APPLICATION & EXPANSION OF THE CPNI RULES

JUSTIN S. BROWN[1]

INTRODUCTION

As the first and last mile conduit, mobile (wireless) and fixed (wired) broadband Internet access service providers (ISPs) play an important role for consumers to access an array of information, services, and applications. As the FCC has taken new steps to preserve an open Internet within the network neutrality debate, concerns nevertheless arise over what extent user privacy is protected by broadband ISPs, social media sites, and apps providers. Thus far, most digital privacy rights that consumers enjoy are guided by terms of service or use conditions that define the extent to which their information is collected and shared.[2] Within this realm, typically consumers willingly agree to broad terms of service agreements[3] that facilitate the big data market, including the first step they take to access the rest of the Internet.

The FCC's 2015 Open Internet Order was significant in its reclassification of broadband as a telecommunications service, in effect

---

[1] Justin S. Brown is an assistant professor in the Zimmerman School of Advertising & Mass Communications at the University of South Florida, teaching courses in telecommunications, law and ethics. His research focuses on telecommunications regulation and broadband policy. He holds a Doctor of Philosophy in Mass Communications and Master of Arts in Telecommunications Studies from the Pennsylvania State University, and a Bachelor of Science in Journalism from the University of Oregon.

[2] Mark A. Lemley, *Terms of Use*, 91 MINN. L.REV. 459, 465–66 (2006).

[3] Nathan J. Davis, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577, 580–82 (2007).

relegating ISPs to fall under Title II common carriage regulation. The FCC used this authority, buttressed by Section 706 and Title III (wireless) to prohibit blocking, paid prioritization, and throttling, and to enhance transparency requirements, noting that important concerns still arise over ISP privacy and data use policies. The FCC initially exercised forbearance to apply the existing customers proprietary network information (CPNI) rules under Section 222. The FCC acknowledged that user data privacy is a legitimate concern and issued separate rules several days before the November 2016 presidential election to specify how CPNI applies to broadband ISPs.[4] As a result of the Republican Administration and the majority that exists within the House, Senate, and the FCC, there is strong speculation that the new broadband privacy rules as well as Title II classification in the Open Internet Order will be significantly weakened.

Concerns over consumer privacy and data use is nothing new within telecommunications policy. In years prior, the FCC has used CPNI rules to protect the confidentiality and disclosure of consumer calling records that apply to wired and wireless telephone and voice over Internet protocol (VoIP) providers. The FCC has also enforced the 1984 Cable Communications Privacy Act to restrict cable television subscriber privacy records, requiring cable operators to refrain from collecting personally identifiable subscriber information without prior consent or to share such information to third parties.[5] However, broadband Internet is arguably an entirely different category in terms of the amount of information that may be collected and shared, moving well beyond telephone numbers and television programming selections to the so-called "Internet of things" ecosystem.

This article describes the development and future of the broadband privacy rules that are an outgrowth of the network neutrality debate and explores the degree to which Section 222 applies to broadband ISP data use and privacy policies. Part I of this article reviews the history of the CPNI rules. Part II of this article explores broadband ISPs and data use and privacy practices to help understand the types of potential information that is collected and shared. Part III examines the CPNI and privacy issues raised as a result of the 2015 Open Internet Order and Title II reclassification. Part IV articulates the FCC's application of the CPNI rules to the Internet, as set forth in the FCC's recent Broadband Privacy Order. In conclusion, Part V discusses the broadband privacy rules likelihood of survival under a new political climate and offers recommendations to further consumer privacy.

---

4 In the Matter of Protecting the Privacy of Broadband and Other Telecommunications Services, Report and Order, FCC 16-148, WC Docket 16-106 (Nov. 2, 2016) ("Broadband Privacy Order").

5 47 U.S.C. § 551 (2017).

PART I: HISTORY OF SECTION 222 & CPNI

The original CPNI rules were passed as part of the Telecommunications Act of 1996 with the notion of trying to prevent incumbent local exchange carriers (ILECs) with competitive advantages in the provision of telecommunication services (InterLATA long distance) rather than a sole focus on privacy.[6]

Eventually the law became more focused on privacy through subsequent interpretations and rulemakings. Under the statute, "every telecommunications carrier has a duty to protect the confidentiality of proprietary information of and relating to other telecommunication carriers, equipment manufacturers and customers"[7] even those who compete in reselling telecommunications services. Telecommunications carriers are prohibited from using proprietary information obtained from another carrier for its own marketing efforts and instead may only use such information in conjunction with providing a telecommunications service.[8]

The statute addresses consumer privacy more specifically, stating that a "telecommunications carrier that receives or obtains CPNI by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable CPNI" [9] in the context of providing telecommunications services. As defined by statute,

'customer proprietary network information' means (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.[10]

CPNI encompasses essential and sensitive calling information including call destination, location, time, and duration. Under the statute, if a telecommunications carrier wants to employ CPNI outside a provision of telecommunications service, it must obtain customer approval prior to "use[ing], disclos[ing], or permit[ting] access to individually identifiable

---

6 *See* Doug Brake, et al., *The FCC's Privacy Foray: Privacy Regulation Under Title II, The Information Technology & Innovation Foundation* (Apr. 2015), http://www2.itif.org/2015-fcc-privacy.pdf (citing Gerald J. Duffy, The New CPNI Rules, Rural Telecommunications, 47 (Mar.-Apr. 2008)).

7 47 U.S.C. § 222(a) (2017).

8 47 U.S.C. § 222(b) (2017).

9 *Id.*

10 47 U.S.C § 222(h)(1) (2017).

CPNI."[11]

In reviewing its legislative history, Section 222 relies on three main consumer protection principles regarding CPNI, including "(1) the right of consumers to know the specific information that is being collected about them; (2) the right of consumers to have proper notice ... such information is being used for other purposes; and (3) the right of consumers to stop the reuse or sale of that information."[12]

More background on congressional intent may be found in early Senate and House versions of the Telecommunications Act of 1996. The Senate's initial version of CPNI in S. 652[13] was aimed at following in the footsteps of the FCC to promote competition and not allow incumbent local exchange carriers to disclose proprietary information they collected with their subsidiary or affiliated company. Nonetheless, they would be allowed to share such information if they obtained customer permission.[14] In contrast, the House version of CPNI in H.R. 1555 focused on consumer privacy protection, establishing the name and initial language of Section 222 and expanding the requirement to all telecommunication carriers. Although Section 104 (a) of H.R. 1555[15] limited the scope of CPNI to "telephone service," the subsequent subsection called for the FCC to study and report to Congress on how emerging, new technologies are impacting consumer privacy, including suggesting further regulations.[16]

As new technologies have evolved to compete with traditional telephone service, the FCC has exercised its authority under Section 222 to expand CPNI requirements to apply to VoIP telephone providers as well as mobile services that offer the equivalent of telecommunications services. In those contexts, the VoIP and mobile providers must protect the privacy of their customers and may not readily share calling information.[17]

Telephone companies must annually certify compliance with the CPNI rules. In terms of enforcement, failure to comply with Section 222 provisions may result in substantial fines by the FCC.[18] The FCC recently

---

11 47 U.S.C. § 222(c)(1) (2017).

12 *See* Dana Grantham Lennox, *Hello is Anybody Home? Deregulation, Discombobulation, and the Decision in U.S. West v. FCC*, 34 Ga. L. Rev. 1645, 1666 (2000) (citing 142 CONG. REC. H1078-03, H1133 (1996)).

13 S. 652, 104th Cong. (1995).

14 *See* Harold Feld, et al., *Public Knowledge, Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World* at 50, (Feb. 2016), https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper(1).pdf (citing S. Rep. No. 104-23, at 22-24 (1995)).

15 H.R. 1555 104th Cong. § 104 (1995).

16 H.R. Rep. No. 104-204, at 90 (1995).

17 FCC Consumer Guide Protecting Your Telephone Calling Records (2015), https://transition.fcc.gov/cgb/consumerfacts/phoneaboutyou.pdf.

18 "Because the CPNI rules provide important consumer protections, the Commission has taken enforcement action against telecommunications carriers and interconnected VoIP providers that were

enforced the CPNI rules against AT&T and reached a $25 million settlement concerning data breaches of 280,000 U.S. customers' names, partial or full social security numbers, and unauthorized access of CPNI.[19] That action was the largest of the five enforcement CPNI-related actions taken by the FCC in 2015, valued at more than $50 million.[20]

PART II: DATA USE & PRIVACY PRACTICES IN THE BROADBAND ISP CONTEXT

For the sake of efficiency, terms of service agreements that contain privacy and data collection principles are more or less "take it or leave it" contracts whereby a customer legally gives up their rights to having their data gathered and shared as specified in the conditions. In general, analysis demonstrates that broadband ISPs terms of service, both in the fixed and wireless context, permit a significant amount of data collection and sharing that currently go well beyond calling information under CPNI.[21]

As one example, Verizon's mobile (wireless) and fixed (wired) broadband users are bound by a common privacy policy.[22] Under the terms set forth, Verizon collects a range of information when using its products and services, including browsing information on the web, wireless location information, as well as the applications, devices, and products that are utilized. Verizon may use this information internally for marketing, network security, and product development and may also aggregate or anonymize this information for marketing purposes including uses by third parties. Verizon will also collect information on users when they visit their websites and may pair wireless and wired browsing information together.[23] Because they involve the web, apps, location, and devices, the above practices go well beyond any data related to the placing of phone calls.

Outside of the Verizon example, there is general consensus that broadband ISPs may collect information beyond customer calling information. This includes the ability to collect information on unencrypted

---

not in compliance with the requirements and we intend to continue to strictly enforce the rules. Companies are reminded that failure to comply with the CPNI rules, including the annual certification requirement, may subject them to enforcement action, including monetary forfeitures of up to $160,000 for each violation or each day of a continuing violation, up to a maximum of 1,575,000." FCC Enforcement Advisory No. 2015-02, *Annual CPNI Certifications due March 1, 2015* (Feb. 9, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-178A1.pdf.

19 *AT&T to pay $25 Million to Settle Consumer Privacy Investigation*, FCC (April 8, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-332911A1.pdf.

20 *Id.*

21 *See e.g.*, Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 SANTA CLARA HIGH TECH. L.J. 483 (2015).

22 *Full Privacy Policy*, VERIZON, http://www.verizon.com/about/privacy/full-privacy-policy (last updated Dec. 2015).

23 *See* Bagley & Brown, *supra* note 20.

Internet traffic,[24] which by some estimates amounts to 65 percent of all downstream Internet traffic in North America.[25] In some instances, an ISP may even employ "deep packet inspection" with unencrypted traffic that allows access to the content of users' activities.[26] Whether encrypted or not, all destination information for Internet traffic may be collected by an ISP[27] because the Internet relies on packet switching and Internet protocol (IP) addresses. Each packet of information, even a request to visit a website, contains the IP address that corresponds to a specific domain name and URL. The ISP is responsible to connect a user to the website through the use of the IP address. ISPs also have the ability to look at how often and how long someone visits a particular website and, in the mobile context, the location of the user.[28] Some suggest too that a broadband ISP will have an even greater ability to collect information with the expansion of the Internet of Things, because many small computers in appliance devices will lack necessary encryption.[29]

PART III: NETWORK NEUTRALITY, TITLE II & PRIVACY IN THE OPEN INTERNET ORDER

To help validate its justification and approach to an open Internet and instill network neutrality provisions,[30] the FCC reclassified broadband Internet access service[31] as a telecommunications service, applying common carrier, Title II classification to both fixed and wireless providers.[32] This particular determination represents a significant shift from previous regulatory classifications that treated broadband Internet access service as an "information service."[33] With an information service

---

[24] Open Technology Institute, *The FCC's Role in Protecting Online Privacy: An Explainer*, 4 (Jan. 2016), https://static.newamerica.org/attachments/12325-the-fccs-role-in-protecting-online-privacy/CPNI__web.d4fbdb12e83f4adc89f37ebffa3e6075.pdf.

[25] *Id.* (citing *Global Internet Phenomena Spotlight: Encrypted Internet Traffic*, Sandvine, 3 (May 8, 2015)).

[26] *See* George Ou, *Understanding Deep Packet Inspection (DPI) Technology*, DIGITAL SOCIETY (Oct. 23, 2009), http://www.digitalsociety.org/files/gou/DPI-final-10-23-09.pdf.

[27] *See* Open Technology Institute, *supra* note 23.

[28] *Id*. at 5.

[29] *See* Feld, et. al., *supra* note 13.

[30] *Federal Communications Commission Record*, FCC Rcd. 15-24, ¶¶ 1-4, (2015).

[31] Broadband Internet access service is "a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all of substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part." *Id.* ¶ 25.

[32] *Id*. ¶¶ 27, 283-84.

[33] "The facts in the market today are very different from the facts that supported the Commission's 2002 decision to treat cable broadband as an information service and its subsequent application to fixed and mobile broadband services." *Id.* ¶ 43.

designation, the FCC would find it difficult to clearly justify any type of CPNI and privacy requirement among broadband ISPs, as there is no explicit mention of privacy concerns raised within the legislative history of Section 706 and "advanced telecommunications capability" under the Telecommunications Act of 1996.[34]

Even though the FCC adopted the telecommunications service classification, its approach is nevertheless common carrier-light as evidenced by its exercise of forbearance authority for twenty-seven different Title II provisions,[35] including no tariffing (rate regulation).[36] The FCC also utilized advanced telecommunications capability under Section 706 to help bolster its common carrier-light approach[37] as well as Title III regulatory jurisdiction to buttress its telecommunications service classification of wireless Internet access service.[38]

Within these foundations, the FCC issued several main network neutrality provisions, retaining the no blocking provisions on "lawful content applications, services, or non-harm devices,"[39] and prohibiting the practice of "throttling,"[40] subject to "reasonable network management."[41] To abate concerns raised by edge providers that some traffic may receive special high-speed lanes,[42] the FCC also barred the practice of "paid prioritization."[43] Instead of restricting commercially unreasonable practices, the FCC created a new rule that prohibits ISPs from unreasonably interfering with or disadvantaging consumers' ability "to reach the Internet content, services, and applications of their choosing"[44] as well as edge providers' access to Internet consumers.[45] These provisions will be applied to make determinations on whether to allow so-called sponsored data plans

---

[34] H.R. Rep. No. 104-458, at 102 (1996) (Conf. Rep.).

[35] *Federal Communications Commission Record*, FCC Rcd. 15-24, at ¶¶ 5, 493 (2015).

[36] *Id.* ¶¶ 41-42, 497-505.

[37] *Id.* ¶¶ 275-82.

[38] *Id.* ¶¶ 285-88.

[39] *Id.* ¶ 15.

[40] Throttling is defined as to "impair or degrade lawful Internet traffic on the basis of Internet content, application, or service, or use of a non-harmful device" *Id.* ¶ 16.

[41] Reasonable network management is defined as "A network management practice is a practice that has a primarily technical network management justification, but does not include other business practices. A network management practice is reasonable if it is primarily used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service." *Id.* ¶¶ 32, 215.

[42] *Id.* ¶¶ 20, 80

[43] "'Paid prioritization' refers to the management of a broadband provider's network to directly or indirectly favor some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management, either (a) in exchange for consideration (monetary or otherwise) from a third party, or (b) to benefit an affiliated entity." *Id.* ¶ 18

[44] *Id.* ¶ 135.

[45] *Id.*

by ISPs[46] and data caps that meter and tier the amount of downloading.[47]

In addition to outlawing blocking, throttling, and paid prioritization, the FCC also further enhanced its existing transparency provisions contained in the Open Internet Rules for end users and edge providers.[48] Broadband providers are now required to disclose promotional rates, all fees and/or surcharges and include specific information on all data caps or allowances in their terms of service.[49] In addition, to help end users be better informed, broadband providers must include packet loss as a measure of network performance.[50] Customers must also be notified when a network practice may be likely to significantly impact their use of broadband Internet access.[51] With respect to the format and nature of required disclosure to consumers, the FCC declined to require separate disclosures for end users and edge providers[52] but established a "safe harbor" process for broadband providers to help aid in the effective presentation of required information.[53]

The FCC acknowledged the importance of privacy concerns, recognizing broadband ISPs are a "necessary conduit for information passing between an Internet user and Internet sites or other Internet users, and are in a position to obtain vast amounts of personal and proprietary information about their customers."[54] It is within this acknowledgment, Title II, and transparency that the FCC's ability to regulate broadband ISP privacy exist, namely through the CPNI requirements under Section 222.[55] Under these provisions, individual subscribers must have their private confidential information that is collected through their relationship as a customer protected by telecommunications carriers and carriers may not use, disclose, or permit access to CPNI information without consent.[56] However, the Commission suggested forbearing its existing CPNI rules that are based primarily on voice wireline phone services because they "do not address many of the types of sensitive information to which a provider of broadband Internet access service is likely to access"[57] including items like a user's web browsing information. The FCC believes that "if consumers have concerns about the privacy of their personal information, such

---

46 *Id.* 151, 152.
47 *Id.* 153.
48 *Id.* ¶ 24.
49 *Id.* ¶¶ 24, 161.
50 *Id.* ¶¶ 24, 166.
51 *Id.* ¶¶ 24, 169.
52 *Id.*¶ 177.
53 *Id.* ¶¶ 24, 179-81.
54 *Id.* ¶ 463.
55 *Id.* ¶462.
56 *Id.*
57*Id.* ¶ 467.

concerns may restrain them from making full use of broadband Internet access services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand."[58] The Commission also found section 706 may not provide enough adequate privacy protections on its own and is on more solid footing under Section 222 to evaluate and enforce requirements.[59]

Several months after the Open Internet Order, the FCC reaffirmed its commitment to broadband privacy by issuing an enforcement advisory that states Section 222 CPNI requirements will be applied to and enforced among broadband ISP providers.[60] The FCC urges all providers to "take reasonable, good-faith steps to comply with Section 222"[61] and "employ effective privacy protections consistent with their privacy policies and core tenets of basic privacy protections."[62] The FCC subsequently initiated a separate rulemaking proceeding to best determine how CPNI rules apply to broadband ISP providers.[63]

Upon a legal challenge to the 2015 Open Internet Order, the D.C. Circuit Court of Appeals, by a 2-1 ruling, upheld the FCC's reclassification of broadband Internet access service from an information service to a telecommunications service.[64] This included sustaining the FCC's finding that both fixed and mobile ISPs should be classified as a telecommunications service[65] and subject to no blocking, no throttling, and no paid prioritization provisions.[66] The D.C. Circuit also rejected claims that the Open Internet rules violate the First Amendment[67] and affirmed the FCC's ability to selectively forbear from applying Title II provisions.[68] While the Court did not address broadband privacy rules specifically, the decision reaffirms the FCC's authority to carry out Title II obligations on broadband ISPs that go beyond network neutrality rules, including the application of CPNI rules.[69]

---

58 *Id.* ¶ 464.

59 *Id.* ¶ 465.

60 Open Internet Privacy Standard, Public Notice, FCC Enforcement Advisory No. 2015-03 (May 20, 2015), https://www.fcc.gov/document/isps-should-take-reasonable-steps-protect-privacy.

61 *Id.* at 2.

62 *Id.*

63 *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 2500 (proposed 2016).

64 United States Telecom Ass'n v. FCC, 825 F. 3d 674 (D.C. Cir. 2016).

65 *Id.* at 695.

66 *Id.* at 675.

67 *Id.*

68 *Id.*

69 *Id.*

PART IV: FCC'S APPLICATION OF CPNI RULES TO BROADBAND ISPS

In November 2016, the FCC issued its Protecting the Privacy of Customers of Broadband and Other Telecommunications Services Order (herein "Broadband Privacy Order") that sets forth new rules concerning how Section 222 (CPNI requirements) of the 1996 Telecommunications Act applies to broadband ISP providers.[70] The FCC reemphasized that Section 222 aims to protect the privacy of data that telecommunications carriers collect from their customers in the provisioning of telecommunications services.[71] The rules are a response to the 2015 Open Internet Order that reclassified broadband internet access service as a telecommunications service,[72] and therefore gives the FCC authority to promulgate the rules under Title II of the Communications Act.[73]

The broadband privacy rules recognize that ISPs possess the ability to monitor their customers' unencrypted and encrypted online activity.[74] Because users must always go through their provider to connect and use different sites and apps on the Internet, broadband ISPs have "access to vast amounts of information" about their customers[75] as a "gatekeeper" that "can collect 'an unprecedented breadth' of electronic personal information."[76] The FCC believes this ability is greater than that of edge providers (e.g. single website or app) who are more limited in accessing a user's Internet browsing activity.[77]

The rules emphasize giving consumers "the tools they need to make informed choices about the use and sharing of their confidential information by their broadband providers,"[78] and center on the following three core principles:

Transparency: Consumers knowing what personal information is collected and how it is employed and shared in terms that are not only accurate, but easily understandable and accessible.[79]

Choice: Consumers exercising rights over what personal data is used and shared by their broadband provider, including establishing opt-in approval for sensitive private information and opt-out approval for non-sensitive data.[80]

---

70 *See* "Broadband Privacy Order" *supra* note 3.
71 *Id.* ¶¶ 21-3.
72 *Id.* ¶ 26.
73 *Id.* ¶ 23.
74 *See* "Broadband Privacy Order" *supra* note 3.
75 *Id*. ¶ 2.
76 *Id*. ¶ 28.
77 *Id*. ¶ 30.
78 *Id*. ¶ 3.
79 *Id*. ¶ 8.
80 *Id*. ¶ 9.

Data Security and Breach Notification: Broadband providers have a duty to safeguard consumer's private information that it collects and maintains, including establishing reasonable measures to secure personal data and notification requirements in circumstances involving a data breach of personal information.[81]

Where there is a data breach, broadband providers must contact customers, the FCC, the Federal Bureau of Investigation, and U.S. Secret Service (in instances of affecting more than 5,000 individuals).[82]
Under the rules, broadband providers are limited in the amount of information they may collect, use, and share without customer permission. In giving consumers choice and control over their personal information, the rules distinguish between sensitive and non-sensitive customer information with different stipulations in terms of consent.[83] Sensitive customer personal information requires express opt-in consent before such data is used and shared,[84] and includes, at a minimum, financial information; health information; social security numbers; precise geo-location information; information pertaining to children; content of communications; call detail information; and a customer's web browsing history, application usage history, and their functional equivalents.[85]

Using or sharing non-sensitive customer personal information requires (at a minimum) opt-out consent,[86] though broadband providers may establish opt-in consent practices for this type of data.[87] In addition, in instances of providing and marketing broadband service, no additional consent is needed outside the initial customer-broadband provider terms of use agreement.[88] Broadband providers are allowed to use and share data for marketing purposes of either their own or their affiliated communications-related services unless a consumer affirmatively opts-out.[89]
Because CPNI only applies to telecommunications services, the rules only affect the privacy practices of broadband ISPs and do not address websites, social media, or edge services.[90] Instead, the FCC clarifies that these entities are governed by rules under the authority of the Federal Trade

81 *Id*. ¶¶ 10-11.
82 *Id.* ¶ 11.
83 *Id.* ¶ ¶ 166, 172.
84 *Id.* at ¶ ¶ 167, 172.
85 *Id.* at ¶ 177. For more justification on the construction of these categories, see ¶¶ 177-91.
86 *Id.*
87 *Id.* at ¶ 172.
88*Id.* at ¶ 203.
89*Id.*
90 *Id.* ¶ 40.

Commission (FTC).[91] The broadband privacy rules also keeps notice and consent intact, meaning even with an expanded CPNI definition, broadband providers have a fail-safe to use or share customer data "for any purpose"[92] just as long as permission is granted by the customer through a terms of use or service agreement.

The FCC significantly expanded the existing definition of CPNI beyond its traditional application that previously covered items like call destination, location, time and duration. "We import the statutory definition of customer proprietary network information (CPNI) into our implementing rules, and define customer proprietary information (customer PI) as including individually identifiable CPNI, personally identifiable information (PII) and content of communications."[93] The FCC justifies its expansion of CPNI in large part because the functionality of broadband Internet access service (BIAS) as a telecommunications service moves beyond the mere placing of voice telephone calls and includes layered data packets of information[94] that may represent an array of various interconnected apps and services.[95] The FCC cites 47 U.S.C. § 222(h)(1)(A), specifically "information . . . made available to the carrier by the customer solely by virtue of the carrier-customer relationship"[96] to "include any information falling within a CPNI category that the BIAS provider collects or accesses in connection with the provision of BIAS."[97]

Within this framework the FCC defines CPNI as "information that BIAS providers and other telecommunications carriers acquire in the connection with their provision of service, which customers have an interest in protecting from disclosure."[98] This includes three specific categories made up of individually identifiable CPNI, personally identifiable information (PII), and content of communications.[99] PII covers information "linked or reasonably linkable to an individual or device"[100] including information (e.g. names, addresses, phone numbers) used to contact an individual.[101] Content of communications refers to "any part of the substance, purport, or

---

91 *Id.* ¶ 87. The FCC does refer to the existing privacy practices previous to broadband reclassification enforced by the Federal Trade Commission (*citing* Fed. Trade Comm'n, Protecting Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, v, vii-ix, 15-22 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf).

92 *See supra* note 56 at 3.

93 *Id.* ¶ 46.

94 *See* ¶¶ 54-62 (describing the different components and layers of an Internet protocol packet).

95 *Id.* ¶ 46.

96 47 U.S.C. § 222(h)(1)(A) (2008).

97 "Broadband Privacy Order," *supra* note 3, ¶ 48.

98 *Id.* ¶ 85.

99 *Id.*

100 *Id.* ¶ 89.

101 *Id.* ¶ 95.

meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose or meaning of a communication,"[102] whether inbound or outbound.[103] This includes, for instance, application payloads of packets that may contain parts of a webpage, email, instant message, video or audio stream, or mapping data.[104] The FCC does provide an exemption to the new rules for CPNI information that has been properly de-identified and may not be reasonably linked to an individual or device. To meet this requirement, the FCC adopted a three-part test articulated by the FTC that includes any attempt to re-identify that data.[105]

While expanding the CPNI definition and application, the FCC also adopted what it deems a "sensitivity-based customer choice framework" that specifically recognizes and offers stronger opt-in consent protections for sensitive customer information, citing FTC support and evidence.[106] The FCC finds that a "sensitivity-based framework better reflects customer expectations regarding how their privacy is handled by telecommunications carriers."[107]

In order to provide consumers with transparency and choice over their customer information, the FCC established guidelines for broadband ISPs to disclose their privacy practices. While not specific to format or style, the FCC does require privacy policies to be "clear, conspicuous, comprehensible and not misleading"[108] in easy-to-understand wording.[109] In terms of substance, notices must contain the following elements: types of customer personal information collected and how it is used, including disclosure;[110] the sharing of customer personal information with affiliates and third parties and how it is used; [111] and customer rights and their privacy choices that specify and describe opt-in and opt-out rights with their personal information.[112] To help in this effort, the FCC directs the Consumer Advisory Committee to develop a proposed standardized notice format. Once approved by the FCC bureaus, providers that voluntarily adopt the Committee's format will be in compliance with the notice clarity requirement.[113] The FCC also sets forth rules on advance notice

---

102 *Id.* ¶ 102.
103 "Broadband Privacy Order," *supra* note 3, ¶ 102.
104 *Id.* ¶ 103.
105 *Id.* ¶¶ 106-110.
106 *Id.* ¶¶ 173, 177-81.
107 *Id.* ¶ 173.
108 *Id.* ¶¶ 147-50.
109*Id.* at ¶ 151.
110 *Id.* at ¶¶ 127-29.
111 *Id.* at ¶¶ 130-31.
112 *Id.* at ¶¶ 132-34.
113 *Id.* at ¶¶ 153-55.

requirements for material changes to privacy policies that give broadband ISP customers the ability to exercise meaningful choice.[114]

Beyond providing greater clarity to privacy notices and protection over sensitive customer information, the Commission also established guidelines requiring broadband ISPs to establish reasonable data security measures[115] as well as data breach notification practices[116] that aim to protect customer data from unauthorized use, disclosure or access. The Commission also prohibited "take-it-or-leave-it" offers that make broadband service contingent on customers surrendering their privacy rights and created heightened notice requirements for financial incentive practices that provide customers with lower monthly rates in exchange for their confidential information.[117]

PART V: THE FUTURE OF BROADBAND CPNI RULES & PRIVACY

Previous to the 2015 Open Internet Order, broadband providers were not governed under the CPNI rules because Internet service was classified as an unregulated information service. Instead broadband providers relied mainly on crafting out data use and privacy policies set forth in terms of use and service agreements and notice and consent enforcement by the FTC. But now, because of Title II classification as telecommunication carriers and the FCC's broadband privacy order, ISPs may be subject to expanded CPNI requirements under Section 222, including new opt-in provisions for the use and sharing of customer's sensitive personal information.

However, a new political reality has taken hold that is likely to curb the proposed expansion of CPNI. The broadband privacy order was released two months prior to the Trump administration taking office and in a political landscape that assumed the FCC and executive branch would remain in democratic control. Already the Trump transition team has goals on weakening regulations and regulatory agencies,[118] including the FCC where there are suggestions that consumer protection and competition functions will be placed with the FTC and net neutrality and Internet

---

114 *Id.* at ¶¶ 156, 163.

115 *Id.* at ¶¶ 235-60.

116 *Id.* at ¶¶ 261-92.

117 *Id.* at ¶¶ 294-303.

118 President Trump signed executive order that requires federal agencies to cut two existing regulations for every new regulation. *See* Bourree Lam, "Trump's 'Two-for-One' Regulation Executive Order, THE ATLANTIC, Jan 30, 2017 at https://www.theatlantic.com/business/archive/2017/01/trumps-regulation-eo/515007/; President Trump signed a different executive order to that directs every regulatory agency to establish regulatory reform task forces that will make recommendations on which regulations to repeal or simplify. *See* David Shepardson and Steve Holland, "In Sweeping Move, Trump Puts Regulation Monitors in U.S. Agencies," REUTERS, Feb. 24, 2017 at http://www.reuters.com/article/us-usa-trump-regulations-idUSKBN1631NV.

privacy rules will be rolled back.[119] Whether through Congress or the Commission, both with their Republican majorities, many believe the network neutrality rules and enforcement will be weakened and reclassification under the 2015 Open Internet Order will be revisited.[120] Certainly if reclassification occurs, the FCC's broadband privacy rules will also be curtailed since CPNI lies within Title II and applies to telecommunications service providers.

Even if network neutrality is not repealed or broadband Internet service is not reclassified, it is likely the FCC's broadband privacy order will be weakened. Newly-appointed FCC Chairman Pai has indicated network neutrality rules were a mistake[121] and the FCC recently suspended the network neutrality transparency requirement for broadband providers with fewer than 250,000 customers and closed an investigation over AT&T and Verizon's zero-rating practices.[122] Chairman Pai also halted enforcement of the first portion of the broadband privacy rules that were set to take effect so it may consider petitions for reconsideration.[123] The FCC may decide not to enforce the order and also decide, whether as part of the petition response, agency reform requirement or a further notice of proposed rulemaking, to alter the rules.[124] Congress may also decide to overturn the rules in the broadband privacy order under the Congressional Review Act or through new legislation.[125]

Outside of the current political climate, upon further legal analysis it is a regulatory reach for the CPNI rules that are contained in the

---

119Alan Pressman, "How the Trump's FCC Team Could Cut Consumer Protection Efforts," FORTUNE, Jan 17, 2017 at http://fortune.com/2017/01/17/trump-fcc/ .

120Klint Finley, "This is the Year Donald Trump Kills Net Neutrality," WIRED, Jan. 2, 2017 at https://www.wired.com/2017/01/year-donald-trump-kills-net-neutrality/.

121 Alina Selyukh, "Trump's Telecom Chief is Ajit Pai, Critic of Net Neutrality Rules," NPR, Jan. 23, 2017 at http://www.npr.org/sections/thetwo-way/2017/01/23/510844936/trumps-telecom-chief-is-ajit-pai-critic-of-net-neutrality-rules.

122Marguerite Reardon, "FCC Chips Away at Net Neutrality Rules," CNET, Feb. 23, 2017 at https://www.cnet.com/news/fcc-net-neutrality-ajit-pai-republican-transparency-rule/.

123 Alina Selyukh, "FCC Chairman Goes After His Predecessor's Internet Privacy Rules," NPR, Feb. 24, 2017 at http://www.npr.org/sections/thetwo-way/2017/02/24/517050966/fcc-chairman-goes-after-his-predecessors-internet-privacy-rules; Groups have petitioned the FCC for reconsideration, including the NCTA – The Internet & Television Association and several advertising trade groups. *See* Doug McPherson, Broadband Carriers, Ad Groups to FCC: Lose the Privacy Rules, RESPONSE MAGAZINE, Jan. 11, 2017 at http://www.responsemagazine.com/direct-response-marketing/news/broadband-carriers-ad-groups-fcc-lose-privacy-rules-9875.

124 Devin Coldeway, "FCC Votes to Negate Broadband Privacy Rules," Tech Crunch, March 1 2017 at https://techcrunch.com/2017/03/01/fcc-votes-to-negate-broadband-privacy-rules/.

125 Larry Downes, "Industry Groups Beg Congress, FCC to Restore Scrambled Internet Privacy Rules," Forbes, Jan 30, 2017 at https://www.forbes.com/sites/larrydownes/2017/01/30/industry-groups-beg-congress-fcc-to-restore-scrambled-internet-privacy-framework/#3e4f10888871.

Telecommunications Act of 1996 to apply to broadband providers. Through examining broadband provider practices (e.g. Verizon) and their ability to collect, use and share information, it is clear that the data collected and shared goes well beyond any previous application of CPNI rules and the telephone context. In fact, one may argue that the amount of personal privacy and information that may be revealed from one's Internet experience vis-à-vis a broadband provider is far greater and more harmful than even the most expansive calling information that CPNI typically pertains to regarding telephone subscribers, namely the numbers, frequency and duration of phone calls.

But what is also clear is that broadband ISPs are already granted consent by consumers in terms of use and service agreements to their current data collection, use and sharing practices that exceed a traditional CPNI interpretation. Customers are also giving permission to have their information shared beyond a typical broadband provider's communications-related service offerings, something that is a requirement already with CPNI rules and those proposed by the FCC.

These facts in and of themselves do not seem to render the FCC's approach to broadband privacy problematic because, whether the CPNI rules are applied or not, most of the requirements set forth in the proposed plan still rely on proper notice and consent. However, a particular concern over the FCC's approach is requiring providers to follow affirmative opt-in provisions from their subscribers with respect to the collection, use and sharing of data that is not related to the provider's broadband or affiliated communication-related services. This specific requirement is different in that most privacy practices in the U.S. may be characterized as an opt-out approach, including many of the existing terms of use and service agreements that applies to the rest of the Internet, whether it's a favorite website, app or edge service.

One incremental approach the FCC may take if it modifies the broadband privacy rules is to tread lightly and shy away from detailing specific practices that are permissible in terms of what data is collected and shared under CPNI, especially beyond managing their broadband or marketing their own affiliated communication services. In contrast to telephone numbers and call logs, the data collected among different parts of the broadband ecosystem is conceivably part of a broadband ISPs data portfolio, including websites, apps, social media traffic, IP addresses and advertising, of which are more analogous to information services and contribute greatly to big data analytics. Likewise such data is also collected and shared among other providers among the various layers of the Internet. It is therefore somewhat unfair to apply the CPNI opt-in rules to broadband Internet access service providers even for sensitive customer personal information, when entities like Google (outside their wireless or

fiber service), Facebook, Netflix and Amazon are not bound by any such provisions and are, arguably in some cases, more aggressive in collecting and sharing data for forms of revenue.

To help protect consumer privacy and still promote competition, the Commission may turn toward a further focus on transparency measures in the broadband privacy order that require clearer notices of data collected, shared and used by broadband providers but aren't over inclusive in terms of expanding the CPNI umbrella. Likewise, the Commission may instill strong measures of accountability, making sure that terms of use and service agreements are accurate and may be enforced with substantial penalties for failure to adequately disclose how a subscriber's information is collected, used and shared. This approach would follow more closely with how the Federal Trade Commission handles privacy issues under Section 5 authority[126] through notice and consent, targeting unfair and deceptive practices to help protect consumers. This approach will also abate legal challenges that would likely rise over an expansion and application of CPNI beyond the telephone context.

Outside of the FCC, concerns over online privacy persist but are part of a larger shift of the commodification of personal data as a revenue stream for companies in exchange for free or inexpensive services.[127] Most consumers also don't readily understand what types of information is collected, used and shared either. Consumers are often willing to agree to terms of use and service agreements even without fully reading or analyzing their meaning[128] or appreciating the ways by which data is gathered.[129] In large part, because of these realities, the very notion of privacy, however one defines it, is contestable in an era of big data and proliferation of digital, connected devices that we rely upon throughout the day to communicate.[130]

While the FCC has tried to tackle broadband privacy through CPNI and Title II authority, one solution is for Congress to clarify how CPNI

---

126 15 U.S.C. §§ 45; FTC, Enforcing Privacy Promises, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

127 See Bagley & Brown supra note 20 at 486.

128 *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1883 (2013). Solove summarizes the cognitive problems as follows: "(1) people do not read privacy policies; (2) if people read them, they do not understand them; (3) if people read and understand them, they often lack enough background to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decision-making difficulties." *Id.* at 1888.

129 Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 260–63 (2013).

130 *See* Ira S. Rubinstein, *Big Data: Then End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74 (2013) ("Big data refers to novel ways in which organizations, including government and businesses, combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising benefits.").

applies to broadband providers. While one may contend the legislative history of CPNI leaves potential room for interpretation, the Internet was not specifically mentioned. In addition, as evidenced by the debate over network neutrality and the 2015 Open Internet Order, Congress has yet to clearly define or establish in a statute that Internet providers offer a telecommunications service and therefore should be classified as telecommunications carriers.

More holistically as we continue to journey into an Internet of Things ecosystem, Congress should address what privacy and security of personal data means in the digital age and define not only its meaning but also specific notice, consent, transparency, accountability and enforcement practices that are consistent throughout the different layers of the Internet. This includes all of the various entities that are connected to the Internet, including not only broadband providers, but also edge services, social media, apps and websites. Regardless of whether the FTC and/or FCC attempts to protect Internet privacy, consumers and the marketplace benefit when there are clear rules of the road and practices established for collecting, using and sharing personal data.