EX PARTE OR LATE FILED

JEFF FLAKE
ARIZONA
SR-413 RUSSELL SENATE OFFICE BUILDING
(202) 224-4521
COMMITTEE ON FOREIGN RELATIONS
COMMITTEE ON
ENERGY AND NATURAL RESOURCES
COMMITTEE ON THE JUDICIARY
COMMITTEE ON AGING

United States Senate

WASHINGTON, DC 20510-0305

STATE OFFICES:
2200 EAST CAMELBACK ROAD
SUITE 120
PHOENIX, AZ 85016
(602) 840-1891

6840 NORTH ORACLE ROAD
SUITE 150
TUCSON, AZ 85704
(520) 575-8633

Accepted / Filed

JUN 8 - 2016

Federal Communications Commission
Office of the Secretary

June 7, 2016

Chairman Tom Wheeler
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: 16-106, "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services"

Dear Chairman Wheeler:

I write in opposition to your proposed rule, "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services." I believe this rule is flawed as a matter of law and policy. It is unnecessary and its existence only made defensible by the FCC's unprecedented reclassification of broadband Internet service providers (ISPs) under Title II of the Communications Act. Worse still, in seeking to solve a problem the FCC created, the rule does so in a burdensome and unconstitutional way.

The process of this rulemaking has also been, at best, wanting. I wrote to you on May 19, along with Senator Boozman, to request that the FCC extend this rulemaking period beyond May 27. You declined this request, arguing that it isn't the FCC's practice to extend comment periods and noting that you expect the rulemaking will have a fulsome record even without the extension. I appreciate your response but still can't help but wonder, why the hurry?

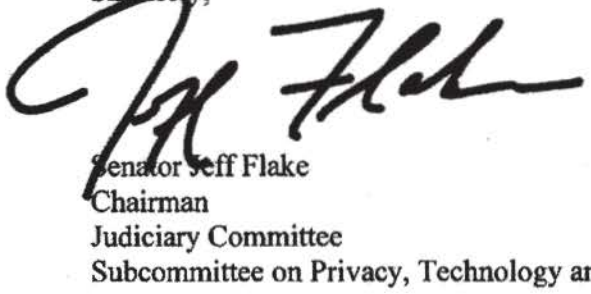
Nevertheless, I am attaching to this letter my comments on the proposed rule. The proposed rule has numerous substantive problems but I would like to focus on one foundational problem with the proposed rule's opt-in requirement for ISP use of so-called customer proprietary information. It appears to me to be an unconstitutional restriction on commercial speech.

The use of customer information for marketing purposes by ISPs is non-misleading protected commercial speech. The restriction of this speech by the FCC does not further a substantial government interest. Even if it did, the means proposed would not directly advance that interest. Lastly, the restrictive opt-in requirement is not narrowly tailored in light of the FTC's longstanding and successful opt-out approach to protecting consumer privacy under Section 5 of the FTC Act. In other words, the proposed opt-in rule completely fails the test set out by the Supreme Court in

No. of Copies rec'd 0 1
List ABCDE

Central Hudson Gas & Electric Corp. v. Public Services Commission of New York, 447 U.S. 557 (1980), and should not be implemented.

Sincerely,



Senator Jeff Flake
Chairman
Judiciary Committee
Subcommittee on Privacy, Technology and the Law

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106

COMMENTS OF SENATOR JEFF FLAKE

I. INTRODUCTION

The Federal Communications Commission (FCC) proposes requiring broadband providers to receive "opt-in" consent from customers before providers share customer information with "non-communications-related affiliates or third parties" or before using this information themselves for non-communications or service-related purposes. This is so, according to the FCC, because "opt-in approval is needed to protect the reasonable expectations of consumers, who may not understand that their broadband provider can sell or otherwise share their information with unrelated companies for diverse purposes (such as targeted advertising), or can repurpose customer information for such purposes."

Importantly, this approach differs in significant respects from that taken by the federal government's primary privacy enforcer, the Federal Trade Commission (FTC). The FTC's approach to data privacy—which covers broadband providers absent Title II reclassification—can be reasonably termed "notice and choice." The FTC encourages companies to provide their customers with proper notice of their privacy practices as well as the possibility of opting out of certain data uses. Opt-in consent is only required for certain very specific forms of sensitive information. This system has allowed consumers to choose how their data are used while providing a regulatory "light touch" that promotes industry innovation.

This difference points to serious constitutional deficiencies in the FCC's proposed rule. Indeed, the rule's opt-in requirement, as proposed, appears to be an unconstitutional restriction on commercial speech.

II. THE PROPOSED RULE WOULD BE AN UNCONSTITUTIONAL RESTRICTION ON COMMERCIAL SPEECH.

The First Amendment to the Constitution protects many forms of commercial speech.[1] Although "[c]urrent doctrine holds that … governmental burdens on this category of speech are scrutinized more leniently than burdens on fully protected noncommercial speech,"[2] the fact

[1] *See, e.g.*, *Morse v. Frederick*, 551 U.S. 393, 446 (2007); *Nike, Inc. v. Kasky*, 539 U.S. 654, 666 (2003) (Breyer, J., dissenting).
[2] *Jordan v. Jewel Food Stores, Inc.*, 743 F.3d 509, 515 (7th Cir. 2014).

remains that commercial speech—including "marketing" speech—"is a form of expression protected by the Free Speech Clause of the First Amendment."[3]

The Supreme Court has articulated a four-part test for evaluating restrictions on commercial speech.[4] *First*, the commercial speech "at least must concern lawful activity and not be misleading."[5] *Second*, the government's interest in curtailing the speech must be "substantial."[6] *Third*, the contemplated regulation must "directly advance[] the governmental interest asserted," and, *fourth*, it cannot do so in a manner "more extensive than is necessary to serve that interest."[7]

The FCC's proposed opt-in rule fails this test across the board. Non-communications and non-service uses of ISP customer data are lawful and not misleading. The FCC's interest in this kind of personal data is not "substantial." Even if it were, it is not clear that the restriction of ISP speech is directly related to advancing that interest, and, regardless, the FTC's effective light-touch regulatory framework shows that an opt-in requirement is more extensive than is necessary to achieve whatever goals the FCC might have.

A. When ISPs use customer data for marketing purposes it is lawful and non-misleading commercial speech.

Speech used for marketing purposes enjoys protection under the First Amendment. This is so because of "the informational function of advertising."[8] For that reason misleading speech enjoys no such protection: "[t]he government may ban forms of communication more likely to deceive the public than to inform it."[9]

A restriction on the use of data for advertising purposes presents constitutional problems. In a 1998 rulemaking under 47 U.S.C. § 222 the FCC attempted to establish opt-in restriction on the targeted-advertising use of Customer Proprietary Network Information (CPNI). When the regulations were challenged in court, the FCC argued that this use-restriction did "not prevent [a phone company] from communicating with its customers or limit anything that it might say to them."[10] The Tenth Circuit disagreed. "Effective speech has two components: a speaker and an audience. A restriction on either of these components is a restriction on speech."[11] In restricting the advertiser's audience through data use, the FCC was restricting the advertiser's speech.

The same situation applies here. In allowing ISPs to use so-called customer proprietary information (CPI) for marketing purposes only after having obtained affirmative consent, the FCC is employing the same exact kind of marketing-speech restriction. This ISP data-use is entitled to protection under the Constitution.

---

[3] *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 557 (2011).
[4] *See Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557 (1980).
[5] *Id.* at 566.
[6] *Id.*
[7] *Id.*
[8] *Cent. Hudson*, 447 U.S. at 563 (citing *First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765, 783 (1978)).
[9] *Id.*
[10] *U.S. West, Inc. v. F.C.C.*, 182 F.3d 1224, 1232 (10th Cir. 1999).
[11] *Id.* (citing *Va. Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 756–57 (1976)).

B. The FCC does not have a substantial interest in protecting customer proprietary information under § 222.

When the government restricts commercial speech, it must further a substantial government interest. The government's power is thus "more circumscribed."[12]

1. The FCC's generalized interest in privacy does not rise to the level of a substantial interest.

The protection of certain kinds of privacy can be a substantial government interest. For example, the privacy of "consumer credit information" has been deemed substantial.[13] This is so because the Fair Credit Reporting Act makes it relatively clear that Congress expects reporting agencies to safeguard the privacy of consumers in the context of credit information.[14]

At the same time "the concept of privacy ... is multifaceted."[15] Accordingly the Tenth Circuit has cautioned, "The breadth of the concept of privacy requires us to pay particular attention to attempts by the government to assert privacy as a substantial state interest."[16] Whatever privacy interest the government seeks to protect, it must "demonstrat[e] that the state has considered the proper balancing of the benefits and harms of privacy."[17] Thus, for example, "the government must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity."[18] Here the FCC provides no such showing as to why the customer data being restricted furthers a particularized government interest. The best it offers is "the reasonable expectations of consumers" that their privacy will be kept secure, a seemingly inadequate basis for the proposed burdensome requirements.

The D.C. Circuit disagreed with the Tenth Circuit's analysis when evaluating a subsequent CPNI rulemaking, but it mischaracterized the extent of the Tenth Circuit's critique.[19] The D.C. Circuit claimed that the Tenth Circuit discounted "a government interest in protecting against the disclosure of 'information [that] could prove embarrassing, ...'"[20] But of course, that was only one of many possible privacy interests the government could assert—along with avoiding harassment or having information misappropriated for the purposes of theft.[21] These particularized interests are consistent with the D.C. Circuit's "analogous" context of "protecting the privacy of consumer credit information."[22] Consumer credit information can be used for any of the nefarious purposes

---

[12] *Cent. Hudson*, 447 U.S. at 564.
[13] *See Trans Union LLC v. F.T.C.*, 245 F.3d 809, 818 (D.C. Cir. 2001).
[14] *See* 15 U.S.C. § 1681(a)(4) ("There is a need to insure that consumer reporting agencies exercise their grave responsibilities with ... respect for the consumer's right to privacy.").
[15] *U.S. West*, 182 F.3d at 1234.
[16] *Id.*
[17] *Id.* at 1235
[18] *Id.*
[19] *See Nat'l Cable & Telecomms. Ass'n v. F.C.C.*, 555 F.3d 996 (2009) ("*NCTA*").
[20] *Id.* at 1001.
[21] *U.S. West*, 182 F.3d at 1235.
[22] *NCTA*, 555 F.3d at 1001 (citing *Trans Union*, 245 F.3d at 818).

suggested by the Tenth Circuit in *U.S. West*. Thus the protection of consumer credit information is clearly consistent with substantial government interests. This is no generalized privacy interest.

It bears noting that the notice and choice framework the FTC prescribes also satisfies the substantial government interest requirement insofar as there *is* a substantial government interest in fair business practices such as adherence to noticed policies. Hence the importance of *notice* and choice in the FTC approach to privacy. Under this FTC model customers are told how their data will be used, at which point they can chose not to share it. Holding companies to these assurances and notices prevents dishonest business practices, avoiding a far more concrete harm than the FCC's proposed consumer confusion about who does what with customer data.

2. The FCC's invention of customer proprietary information is inconsistent with the concrete privacy interest in CPNI established by Congress in § 222.

Beyond the FCC's asserted generalized privacy interest, the proposed privacy rule aims to apply well beyond CPNI, which exceeds the privacy interest contemplated by Congress in 47 U.S.C. § 222. The statute itself protects CPNI, which is a particular category of information (essentially telephonic metadata).[23] Indeed, the privacy interests the FCC asserted under § 222 in both the 1998 CPNI order (at issue in the Tenth Circuit's *U.S. West*) and the 2007 CPNI order (at issue in the D.C. Circuit's *NCTA*) both sought to prevent the disclosure of CPNI data. The proposed privacy rule at issue here, however, largely applies to a new category of information entirely—consumer proprietary information (CPI)—a category significantly broader than CPNI. The FCC justifies this change by asserting that § 222(a) protects CPI and not CPNI because § 222(a) states, "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of … customers," 47 U.S.C. § 222(a), and "proprietary information of … customers" is different from "customer proprietary network information" as used in § 222(c), (d), and defined in § 222(h)(1).

The statute does not support this interpretation. While "proprietary information of … customers" is textually distinct from "customer proprietary network information," the FCC puts more weight on this distinction than the text can bear. To begin with "proprietary information of … customers" is clearly not a term of art.[24] Terms of art are "concepts that are 'well understood' at the time of a statute's enactment."[25] With such terms of art "Congress obviously intend[s] to incorporate its supposedly well-established meaning" into a statute.[26] There was no "well-established meaning" for the term "proprietary information of … customers" at the time of the

[23] 47 U.S.C. § 222(h); *see e.g.* 47 U.S.C. § 222(h)(1)(A)("[I]nformation 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 ….").

[24] If anything, the term of art in § 222(a) would be "confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers," and the FCC does not claim to gloss such an obviously unwieldy phrase.

[25] *Bernardo ex rel. M & K Eng'g, Inc. v. Johnson*, 814 F.3d 481, 488 (1st Cir. 2016) (quoting *Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995)).

[26] *Id.*

statute's enactment, as demonstrated by the fact that it does not seem to have been defined as a unique term until the FCC's 2014 *TerraCom NAL*.[27]

Thus § 222(a) is best read in conjunction with § 222(d), which states "Nothing *in this section* prohibits a telecommunications carrier from using, disclosing, or permitting access to *customer proprietary network information* obtained from its customers ...."[28] The exceptions provided by § 222(d) for CPNI use apply across the statute including § 222(a). Using a proper reading, § 222(d)'s CPNI exceptions apply to the "proprietary information of ... customers" in § 222(a), otherwise the exception in § 222(d) would not apply to the statute's operative language even though the text of § 222(d) applies to "this section." Any contrary reading, where CPI is not CPNI, would mean that Congress intended § 222(d) to apply to the entire statute except for its operative clause, which runs contrary to the Harmonious-Reading Canon and the presumption that "intelligent drafters do not contradict themselves."[29]

C. Any FCC interest in personally identifiable information is not directly served by restricting the speech of ISPs.

Even if, *arguendo*, the FCC has a substantial interest in protecting CPI, regulating data use by ISPs does not directly serve that goal. Once a substantial interest is identified, "the restriction must directly advance the state interest involved."[30] Thus, for example, there is a direct relationship between promoting energy conservation and restricting electric power advertisement because "[t]here is an immediate connection between advertising and demand for electricity."[31] On the other hand, the FCC's 1998 CPNI rule was held not to be directly connected to the asserted interest because the court had "no indication of how [the disclosure of sensitive and potentially embarrassing personal information] may occur in reality with respect to CPNI."[32]

Here the FCC proposes to advance its interest in protecting privacy against ISPs under a theory that they are uniquely positioned to have access to sensitive information. Like the thousand-eyed Argus of mythology, ISPs are supposed to be the all-seeing watchmen of our personal information according to the FCC's view. Indeed, "ISPs are 'in a position to develop highly detailed and comprehensive profiles of their customers—and to do so in a manner that may be completely invisible.'"

But this alleged threat to privacy is wholly theoretical. The FCC points to no patterns of abuse by ISPs of their customer information, let alone the kind of particularized abuse that could properly rise to a significant government interest. In fact there doesn't seem to have been any: the FTC, regulating ISPs prior to the Title II reclassification for over a decade, has never brought a privacy enforcement action against ISPs. Insofar as the FCC has a substantial interest in customer privacy, regulating ISPs is not a direct way to address actual privacy threats.

---

[27] *TerraCom, Inc. and YourTel Am., Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd. 13325 (2014).
[28] 47 U.S.C. § 222(d) (emphasis added).
[29] Antonin Scalia & Bryan Garner, Reading Law 180 (2013).
[30] *Cent. Hudson*, 447 U.S. at 564.
[31] *Id.* at 569.
[32] *U.S. West*, 182 F.3d at 1237.

The threat is not only theoretical, but also faulty. A recent report by Georgia Tech professor Peter Swire, the architect of HIPAA, refutes any claims that ISPs are uniquely suited to gain access to personal information. As Prof. Swire has noted, "[U]sers today often connect to the Internet with multiple devices and from multiple locations, and at far higher speeds. This means that any single ISP views a diminishing portion of a user's Internet activity, and that the portion they do not carry represents an enormous and growing volume of data and transactions."[33] Furthermore, "[w]ith encrypted content, ISPs cannot see detailed URLs and content even if they try."[34] By the end of the year it's expected that 70% of web traffic will be encrypted.[35] Not only do users use multiple ISPs to transfer their increasingly encrypted data, but "widespread use of Virtual Private Networks … and third-party proxy services, are further limiting ISP visibility."[36] The FCC has not refuted these claims.

Thus, insofar as the FCC has any general or particularized substantial interest in customer privacy, regulating ISPs is not a direct way to address actual privacy threats either practically or theoretically.

D. The FTC's effective approach to data protection is a less restrictive way to achieve any substantial interest the FCC might have in restricting the speech of ISPs.

The FCC's proposed rule would *still* fail even if it directly furthered a substantial interest because the FTC's effective enforcement regime is less restrictive than the FCC's onerous opt-in rule. The final question in testing a restriction on commercial speech is whether the action "is no more extensive than necessary to further the State's interest. …"[37] There must be "a fit" between the end and the means.[38] While this doesn't mean that the government needs to "employ the least restrictive means" it does need to "utilize a means that is 'narrowly tailored' to its desired objective."[39] Indeed, "The availability of less burdensome alternatives to reach the stated goal signals that the fit between the legislature's ends and the means chosen to accomplish those ends may be too imprecise to withstand First Amendment scrutiny."[40]

In *Central Hudson* the government failed in large part because it had "not demonstrated that its interest … cannot be protected adequately by more limited regulation of [Central Hudson's] commercial expression."[41] Similarly in *U.S. West* the Tenth Circuit observed in dicta that "the FCC's failure to adequately consider an obvious and substantially less restrictive alternative, an

---

[33] Peter Swire, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* 23 (The Institute for Information Security & Privacy at Georgia Tech, Feb. 29, 2016), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf.
[34] *Id.*
[35] Rick Boucher, Level the Privacy Playing Field to Protect Consumers, *The Bureau of National Affairs, Inc.* (Mar. 28, 2016), http://www.bna.com/level-privacy-playing-n57982069099/.
[36] Swire, *supra*, at 23.
[37] *Cent. Hudson*, 447 U.S. at 569–70.
[38] *U.S. West*, 182 F.3d at 1238.
[39] *Id.* (quoting *Bd. of Trs. of the State Univ. of N.Y. v. Fox*, 492 U.S. 469, 480 (1989)).
[40] *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 529 (1996) (O'Connor, J., concurring).
[41] *Cent. Hudson*, 447 U.S. at 570.

opt-out strategy, indicates that it did not narrowly tailor the CPNI regulations regarding customer approval."[42]

The FCC's approach is not narrowly tailored at all. Instead, it is broad and restrictive. First and foremost, it imposes an opt-in requirement on non-communications and non-service related CPI use. An opt-in requirement "requires that the [ISPs] obtain from the customer affirmative, express consent allowing the requested usage, disclosure, or access to the covered information after the customer is provided appropriate notification of the provider's request…." The ISP cannot use the covered information without obtaining the affirmative consent of a customer. In other words, to protect customer privacy the FCC will not let the ISPs engage in certain kinds of targeted marketing unless the customers expressly allow for it.

Compare this to the approach taken by the FTC. Under the FTC's enforcement power it has adopted a notice and choice framework to protect privacy.[43] Under this framework, the FTC maintains that data collectors must disclose their data-collection practices to customers, at which point customers should have options with respect to how their personal information may be used. In practice this typically means that customers should be given the chance to opt-out of data use. While the FTC's most recent privacy report supports opt-in consent for "sensitive data for certain purposes," this is not the general rule, and indeed only applies to "information about children, financial and health information, Social Security numbers, and precise geolocation data."[44]

The FTC's opt-out framework satisfies any substantial interest the government might have in protecting privacy. During a recent hearing, Chairwoman Ramirez of the FTC was asked whether in her view, "the FTC's privacy protection regime over the years has been sufficient to effectively protect consumers' rights as it relates to ISPs?" Chairwoman Ramirez responded, "I think the Federal Trade Commission has done a very effective job in addressing consumer privacy and ensuring that consumer information is appropriately safeguarded." Republican Commissioner, Maureen Ohlhausen, agreed, observing, "I do think the FTC has been very effective. We've had a long history of bipartisan support. We've brought well over 100 cases in this area." The FCC has not explained why Chairwoman Ramirez and Commissioner Ohlhausen are wrong to think this or why a more stringent opt-in regime is necessary. Thus the agency has "not demonstrated that its interest … cannot be protected adequately by more limited regulation of [ISPs'] commercial expression" because they exist and have clearly been adequate until this point.

It is the case that the D.C. Circuit concluded that the 2007 CPNI opt-in requirement satisfied this final *Central Hudson* prong. It is difficult in practice to agree with that court's conclusion that opt-out is "only 'marginally less intrusive'" than opt-in for First Amendment purposes.[45] It is clear

---

[42] *U.S. West,* 182 F.3d at 1239–40.

[43] *See generally* Federal Trade Comm'n, Privacy Online: Fair Information Practices in the Electronic Marketplace, Report to Congress (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[44] Federal Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change, Federal Trade Commission 59 (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[45] *NCTA*, 555 F.3d at 1002 (quoting *Trans Union Corp. v. F.T.C.*, 267 F.3d 1138, 1143 (D.C. Cir. 2001))(internal quotation marks omitted).

that the effects of opt-in on the ability of providers to reach consumers for marketing purposes are severe. Indeed, if the result of opt-in versus opt-out were six of one, half-dozen of the other, this whole exercise would seem pointless. The effect—if not the goal—of opt-in is to restrict the use of customer data for marketing purposes more than opt-out. At minimum, the FCC bears the burden of proving that opt-in is only marginally more intrusive and, until such time as it meets that burden, it should act consistently with the Tenth Circuit, which held that an opt-out regime does represent a significantly less intrusive regulation of protected speech.

The D.C. Circuit decision, however, is distinguishable from the situation we confront in this rulemaking because it involved CPNI—not the new category of CPI. There the court relied largely on the FCC's administrative record to justify its opt-in regime for CPNI. Here the FCC has conducted no studies on the need for opt-in. It offers no real findings on the subject. It points to no outside research justifying its proposed restrictions. When the FTC planned to issue *a report*—not a rule—on privacy in 2012 it conducted a series of workshops with privacy experts, advocates, and industry stakeholders. It then issued a draft staff report and took comments before adopting a final Commission report. By contrast in preparing for this, *a rule*, the FCC held one workshop a year ago, issued a complex NPRM asking over 500 questions of stakeholders, and has tenaciously adhered to an arbitrary commenting deadline against the protests of diverse stakeholders and a bipartisan majority of Commissioners. So onerous a rule as opt-in cannot be supported by so scant a record as presented here.

Furthermore, in *NCTA* the D.C. Circuit held that the FCC's opt-in rule for CPNI was justified because the agency "reasonably concluded that customer information would be at a greater risk of disclosure once out of the control of the carriers and in the hands of entities not subject to 222."[46] However, by "subject to 222" the court referred to CPNI, which is a particular and narrow set of information established by statute and over which third parties have no clear legal obligations. The proposed rules here deal with a new category of CPI data which is much broader than CPNI and is already covered by the FTC's opt-out rules for any third parties. Thus in applying an opt-out regime to the protection of CPI the FCC would be treating like information in a like manner between both the providers (as regulated by the FCC) and the third parties (as regulated by the FTC). Indeed, Chairman Wheeler himself has recognized the wisdom of treating like information in like manners between providers when he testified before the House that the FCC "will not be regulating the edge providers differently" from ISPs.[47]

III. CONCLUSION

While it might be too much to ask that the FCC abandon the folly that is its crusade to regulate the Internet through common-carrier reclassification, it should at least adopt the light-touch, opt-out approach to data privacy employed by the FTC. This will not solve the further constitutional problems presented by placing onerous privacy regulations on ISPs in order to

---

[46] *Id.* Here, of course, the FCC is not just requiring opt-in for providing CPI to third-parties, but rather restricting the use of CPI *by ISPs* for non-communications marketing. This alone makes the opt-in restriction here more severe than that which the court upheld in *NCTA*.

[47] *Oversight of the Federal Communications Commission Before the H. Subcommittee on Communications and Tech.*, 114th Cong. 141 (Nov. 17, 2015) (statement of Tom Wheeler, Chairman of the F.C.C.).

advance a vague commitment to privacy that is not born by the text of § 222, but it will be a step in the right direction. And it will avoid doing unnecessary damage to our vibrant and innovative Internet ecosystem.