Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

REPLY COMMENTS OF PUBLIC KNOWLEDGE, BENTON FOUNDATION, CENTER FOR DIGITAL DEMOCRACY, CONSUMER ACTION, WORLD PRIVACY FORUM, CONSUMER FEDERATION OF CALIFORNIA, CONSUMER FEDERATION OF AMERICA AND NATIONAL CONSUMERS LEAGUE

Harold Feld
Ryan Clough
Meredith Rose
Kerry Sheehan *
Dallas Harris
John Gasparini
PUBLIC KNOWLEDGE
1818 N St. NW, Suite 410
Washington, DC 20036
(202) 861-0020

Amina Fazlullah
Benton Foundation
1625 K St NW
Suite 1100
Washington, DC 20006

Jeffrey Chester
Center for Digital Democracy
1621 Connecticut Ave NW
Suite 500
Washington, DC 20009

Linda Sherry
Consumer Action
1170 Market Street
Suite 500
San Francisco, CA 94102

Richard Holober
Consumer Federation of California
1107 9th St.
Suite 625
Sacramento, CA 95814

Beth Givens
Privacy Rights Clearinghouse
3033 Fifth Ave.
Suite 223
San Diego, CA 92103

Susan Grant
Consumer Federation of America
1620 I Street, NW
Suite 200
Washington, DC 20006

John Breyault
National Consumers League
1701 K St NW
Suite 1200
Washington, DC 20006

Pam Dixon
World Privacy Forum
3108 Fifth Ave.
Suite B
San Diego, CA 92103

*Bar admission pending

July 6, 2016

Public Knowledge, the Benton Foundation, the Center for Digital Democracy, Consumer Action, the World Privacy Forum, the Consumer Federation of California, the Consumer Federation of America, and the National Consumers League hereby file these timely Reply Comments in the above captioned proceeding.

SUMMARY

Opponents of the Commission's proposed rules rely primarily on two flawed arguments. First, they characterize the purpose of the Commission's privacy authority[1] as focused solely on the question of disclosure to third parties. But Congress intended far more under the basic rubric of "privacy." As the D.C. Circuit stated in *NCTA v. FCC*: "There is a good deal more to privacy than that … 'both the common law and the literal understandings of privacy encompass the individual's control of information concerning her person.'"[2] As discussed in greater detail below, Congress has already determined that when an entity engaged in either telecommunications services or provision of video services ***uses*** information in an unauthorized manner, regardless of whether the information is exposed to third parties, the ***use*** causes harm to the subscriber and conveys an unwarranted windfall on the operator.

Accordingly, even assuming that "anonymization" is both genuinely feasible[3] and enforceable, this would only mitigate the potential harm, not eliminate it. In the plain language of Section 222, Congress made it clear that it considered only aggregate information, not anonymized information, as appropriate for use without consent.[4] Congress defined "aggregate information" in a way that expressly prohibits data relevant to only a single individual, rejecting

[1] 47 U.S.C. §§ 222, 338(i), 551 and 605.
[2] *NCTA v. FCC*, 555 F.3d 996, 1001 (D.C. Cir. 2009) (quoting *U.S. Dep't of Justice v. Reporters Comm'n for Freedom of the Press*, 489 U.S. 749, 763 (1989)).
[3] *Cf.* Comments of Open Technology Institute at New America at 21–22.
[4] 47 U.S.C. § 222(c)(3).

anonymization of an individual's data as sufficient.[5] The Commission should therefore reject proposals to permit use or disclosure to third parties of anonymized individual data.

The second flawed argument that pervades opponents' comments is the assertion that the proposed rules amount to content-based regulations of speech that violate the First Amendment. To the extent the proposed regulations implicate the First Amendment at all, they are properly evaluated under the ordinary framework for commercial speech, and do not trigger a heightened level of scrutiny.[6] The statute and proposed regulations are content neutral, despite the efforts of commenters to find discrimination among speakers or messages in the Commission's proposals.

Furthermore, the effort to manufacture a "content-based" distinction proves too much from the perspective of these commenters. If they are correct that any distinction made in the use of customer information is impermissible content discrimination, then the proposals of commenters—that the Commission should adopt the approach of the Federal Trade Commission (FTC), which considers such factors as the nature and type of information in determining what level of protection to afford[7]—are equally unconstitutional. Furthermore, even if the Commission accepts the carrier argument that the First Amendment applies to their business activities of data harvesting, and further agrees with the carriers that requiring "opt-out" for certain activities and "opt-in" for others creates a content-based distinction triggering heightened scrutiny, the natural resolution is to adopt a uniform opt-in policy, consistent with the direct instructions of Congress in Section 222.[8]

---

[5] 47 U.S.C. § 222(h)(2).
[6] *See Verizon California Inc. v. FCC*, 555 F.3d 270, 274–75 (D.C. Cir. 2009).
[7] *See* Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission at 3–6.
[8] It should be noted that under the First Amendment analysis championed by Tribe and others, Section 222(b) creates a First Amendment conflict by treating rival carriers differently than other potential rivals. This would require a finding that *Sorell* directly overrules the D.C. Circuit's

ARGUMENT

I. The FCC'S Privacy Protection Authority Consistently Addresses the Unauthorized Use of Personal Information, Not Merely the Disclosure of Unauthorized Information.

For the most part, opponents of the Commission's proposal simply reiterate arguments that Public Knowledge addressed in its privacy white paper[9] and initial comments.[10] [cite] One particular point, however, appears to require further clarification. Parties in support of permitting use of "anonymized" data generally argue that the statute seeks solely to protect consumers from exposure of their information to third parties.[11] Likewise, Commenters lamenting that the Commission fails to consider the supposed benefits from violating a user's privacy and failing to disclose this fact oddly fail to explain why – if the benefits are so manifestly clear – they cannot comply with straightforward disclosure rules and seek explicit permission. Similarly, commenters that insist that there is no harm in disclosure ignore that it is Congress that has determined the harm, not the Commission.[12]

---

decision in *Verizon California*. It would also eliminate a significant pro–competitive regulation on which commenters who support this interpretation of *Sorell* depend.

[9] *See* Public Knowledge, Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World (Feb. 2016), available at https://www.publicknowledge.org/documents/protecting-privacy-promoting-competition-white-paper.

[10] *See generally* Public Knowledge Comments.

[11] *See* AT&T Comments at 5.

[12] There is a certain irony in light of Comcast's claims both with regard to the track record of ISPs, the incentive of ISPs to protect customer information, and the lack of consumer harm. As documented in the settlement agreement between Comcast and the California Public Utility Commission (CPUC), Comcast is responsible for what is probably the longest ongoing data breach and privacy violation by an ISP on record. *See Comments of Greenlining Institute and Media Alliance*. For three years, Comcast was aware that it was exposing the unlisted phone numbers of VOIP subscribers to the public interest – resulting in some cases in death threats and stalking. Despite this direct knowledge of the data breach, and the terrible toll it took on the lives of some of its customers, Comcast did nothing until the California legislature passed a law it hoped would grant it immunity from CPUC prosecution.

A. Congress Intended to Give Consumer's Control Over The Personal Information They Expose To Providers of Telecommunications Services.

Congress most explicitly directed the FCC to ensure that users are not merely protected from exposure to third parties, but can actively control how the telecommunications provider itself ***uses*** the information. Even in the original initial privacy statute included in the Communications Act of 1934[13] (which copied the provision from the Federal Radio Act of 1927),[14] Congress prohibited carriers not merely from "publish[ing]" or "divulge[ing]" the contents or information relevant to the communication, it also expressly prohibited any carrier or third party "not authorized thereto" from benefiting from the information.

Since this initial prohibition on unauthorized ***use*** of information relating to a communication, in addition to simply exposing the information to third parties, Congress has repeatedly made clear its legislative judgment that consumers are entitled to control not merely publication, but ***use*** of information – and to enjoy meaningful notice as a pre-condition for consent. The Cable Privacy Act explicitly requires cable providers to provide detailed information on the intended use of any personal information, and prohibits the cable operator from even collecting such information (let alone use or disclose the information) without first obtaining "written or electronic consent" from the subscriber.[15] Congress enacted an identical provision to give subscribers to DBS services control over their information.[16]

In the Telecommunications Act of 1996, Congress continued to expand the concept of user control as a critical element of the Commission's privacy jurisdiction. Section 222(c) explicitly requires consent of the customer before a carrier can "***use***, disclose, or permit access

---

[13] Communications Act of 1934, § 605, 48 Stat. 1103 (now codified at 47 U.S.C. § 605(a)).
[14] *See* A Legislative History of The Communications Act of 1934, edited by Max D. Paglin Oxford University Press (1989) at 721.
[15] 47 U.S.C. § 551 (a) & (b)(1).
[16] 47 U.S.C. § 338(i)(1) & (3)(A).

to" CPNI.[17] As discussed at length in the Public Knowledge White Paper, the House and subsequent conference adopted rules designed to give consumers direct control over the use of their personal information and to limit the ability of carriers to use the information without consent.[18] As the House Conference Report clearly stated:

> The protections contained in §§ 222(b)-(c) represent a careful balance of competing, often conflicting considerations. ***First, of course, is the need for customers to be sure that personal information that carriers may collect is not misused.***[19]

In short, since passage of the Federal Radio Act in 1927, Congress has always intended that the FCC provide to the users of telecommunications services control over the use of their private information – not merely security from disclosure to third parties. Congress never retreated from this substantial government purpose, as opponents of the Commission's proposed protections appear to believe. To the contrary, Congress has demonstrated both a clear understanding of the increasingly complex and technical information that communications providers generate in the performance of their functions ***and*** an increased determination to empower consumers to prevent misappropriation of that information ***by*** carriers – regardless of whether or not carriers disclose this information to third parties.

Where Congress has demonstrated a clear and consistent pattern for 90 years, it is not for carriers or the Commission to decide that Congress does not mean what it says. Congress speaks with an increasingly louder and uncompromising voice. Congress entrusted to ***consumers*** – not to carriers or even the Commission -- the power to judge whether or not a specific use of the information collected by a carrier would benefit them. The supposed consumer benefits of touted by carriers to collect consumer information *sub rosa*, the claims that carriers rather than customers know what will serve their customers best do not allow carriers – for all their

[17] 47 U.S.C. § 222(c).
[18] Public Knowledge White Paper at 13-19.
[19] H.R. Rep. No. 104-204 (1995) at 90 (emphasis added).

supposed benevolent wisdom, market incentive and enlightened self-interest – to arrogate to themselves that power which Congress bestowed upon their customers. Nor can the wailings of carriers about supposed competitive disadvantages when they compete in the advertising market, or the insistence that the information is otherwise available, permit carriers or the Commission to rewrite the statute. For 90 years, Congress has unequivocally sought to empower consumers to control their own information. That carriers find this inconvenient to their business plans is insufficient reason to rewrite the statute and usurp from consumers the control that Congress has given them.

B. Recent Data Supports the Importance Of Enhancing Privacy Online Wherever Possible.

Recent data confirms, rather than undermines, the substantial government interest in empowering consumers to control their own information. In May, the National Telecommunications Information Administration (NTIA) released a survey indicating that a significant number of Americans refrain from engaging in online activities ranging from civic engagement to shopping because they fear for their privacy online.[20] Numerous reports from the Pew Research Center emphasize that while consumers often feel conflicted about how to balance privacy and security, they uniformly share a greater desire for better understanding of how private companies collect and use their information and want greater control over corporate collection and use of their data.[21]

---

[20] Rafi Goldberg, "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities" (National Telecommunications & Information Administration, May 13, 2016), available at https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[21] *See* Rafi Goldberg, "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities" (National Telecommunications & Information Administration, May 13, 2016), available at https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities; Lee Rainie, "How Americans balance privacy concerns with sharing personal information: 5 key findings" (Pew Research Center, Jan. 14,

Contrary to the self-interested assertions of privacy opponents, consumers continue to regard the power explicitly granted by Congress in Section 222 to control the use of their information. This ability to have confidence in the privacy of their information, as well as the ability to judge for themselves whether and to what extent to allow carriers to use this information, directly bears on their willingness to adopt and use electronic communications. In light of the express federal policy to encourage widespread broadband deployment and use,[22] there can be no doubt in the continued vitality of the substantial government interest in giving consumers – rather than carriers – control over their own personal information.

II. The FCC's Proposed Rules Need Not Satisfy a Strict or Heightened Level of First Amendment Scrutiny, Above the Ordinary Requirements for Regulations of Commercial Speech.

In various comments filed in these proceedings, ISPs and industry representatives contend that the consumer privacy protections proposed by the FCC (the "Proposed Rules") would violate the First Amendment to the United States Constitution.[23] These legal arguments either overextend free speech doctrines to predict heightened judicial scrutiny for illusory "content-based" distinctions in the Proposed Rules, or they misapply the well-established framework for evaluating governmental restrictions on commercial speech, from *Central Hudson*

2016), available at http://www.pewresearch.org/fact-tank/2016/01/14/key-findings-privacy-information-sharing/; Lee Rainie and Shiva Maniam, "Americans feel the tension between privacy and security concerns" (Pew Research Center, Feb. 19, 2016), available at http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/.

[22] *See, e.g.*, The Broadband Data Improvement Act of 2008, Pub. L. 110-385.

[23] *See* Laurence H. Tribe and Jonathan S. Massey, "The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment," submitted jointly by National Cable & Telecommunications Association, United States Telecom Association, and CTIA (hereinafter, "Tribe & Massey") at 1–8; Comments of AT&T at 91–100; Comments of Comcast at 87–100; Comments of Verizon at 36–40; Comments of CTIA at 73–94; Comments of the United States Telecom Association at 31–32.

Gas & Electric Corp. v. Public Service Comm'n of New York.[24] The Commission should not be dissuaded from adopting the Proposed Rules on either count.

A. The Distinctions in the Proposed Rules Do Not Trigger Heightened Scrutiny.

Many of the commenters raising constitutional challenges to the FCC's proposed privacy rules are vague about precisely what in the regulated conduct qualifies, directly or indirectly, as speech warranting protection from the First Amendment.[25] This is not surprising, given that any constitutional challenge to the rules will likely be evaluated in the context of specific applications.[26] However, the most prevalent theory among opponents seems to be that the Proposed Rules will burden marketing communications that would otherwise rely upon CPNI to target an audience of particular individual.[27] This is prototypical commercial speech,[28] and thus, to the extent the First Amendment applies at all to the conduct regulated by the Proposed Rules, their "validity [would] be tested according to the standards set forth in *Central Hudson*."[29]

Certain opponents argue that Proposed Rules make "content-based" distinctions among different types of speech—for example, arguing that they "discriminat[e] against certain speakers (ISPs) and against certain subject matter (truthful messages concerning 'non-communications related services')."[30] They therefore suggest that such content-based regulation should trigger strict scrutiny or an otherwise heightened level of scrutiny, above and beyond the ordinary Central Hudson framework.[31]

---

[24] 447 U.S. 557 (1980).
[25] *See, e.g.*, Tribe & Massey at 2.
[26] *Bartnicki v. Vopper*, 532 U.S. 514, 524 (2001) (deciding First Amendment challenge to privacy statute "as applied to the specific facts of these cases").
[27] *See, e.g.*, Tribe & Massey at 4.
[28] *See, e.g., United States v. United Foods, Inc.*, 533 U.S. 405, 409 (2001).
[29] *National Cable & Telecommunications Ass'n v. FCC*, 555 F.3d 996, 1000 (D.C. Cir. 2009).
[30] Comments of AT&T at 92; *see also* Tribe & Massey at 30–31.
[31] *See* Tribe & Massey at 5–6, 14; Comments of CTIA at 76–77; Comments of AT&T at 92.

This contention misreads both First Amendment jurisprudence and the Proposed Rules. "Deciding whether a particular regulation is content based or content neutral is not always a simple task."[32] Following the language of Section 222,[33] most of the Proposed Rules would make no content-based distinctions at all—for example, they would require opt-in consent for all disclosures to third parties, regardless of the content of the information or the intended use by the recipient.[34]

Certain commenters point to the varying restrictions on ISPs' own uses of customer data, such as the requirement of opt-out consent for use the marketing of "communications-related services" versus the opt-in consent required for use in marketing other services.[35] But this distinction is not a government regulation "of speech because of [agreement or] disagreement with the message it conveys," which is the "principal inquiry in determining content neutrality."[36] Instead, the distinction between the marketing of "communications-related services" and other services is based on the implied level of consent that consumers would typically expect for different uses, as opposed to any intent to favor or restrict one type of marketing content over another.[37] Thus, it is plainly "justified without reference to the content of the regulated speech," and strict scrutiny therefore does not apply.[38]

In arguing otherwise, certain commenters misread the Supreme Court's decision in *Sorrell v. IMS Health Inc*. The statute at issue in *Sorrell*, the Vermont Prescription Confidentiality Act, explicitly targeted a particular type of pharmaceutical marketing to doctors,

---

[32] *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 642 (1994).
[33] 47 U.S.C. § 222.
[34] NPRM ¶ 18.
[35] *E.g.*, Tribe & Massey at 30–31.
[36] *Id.* (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)).
[37] NPRM ¶ 18.
[38] *Ward*, 491 U.S. at 791.

with a particular viewpoint (the promotion of brand-name as opposed to generic drugs), by attempting to restrict the availability of commercial data that enabled pharmaceutical companies to deliver such a message.[39] This clear "viewpoint discrimination" was "designed to impose a specific, content-based burden on protected expression," which drove the Supreme Court to invalidate the statute as a violation of the First Amendment.[40] In that context, the Court merely reiterated the long-established holding that, under the First Amendment, the government may not single out some speech for disfavored treatment because it disagrees with its message, regardless of whether it applied the ordinary test for restrictions on commercial speech or some form of "heightened scrutiny."[41] In contrast, there is no plausible argument that the Proposed Rules are designed to either favor or disfavor the messages involved in the marketing of "communications-related services" relative to the marketing of other services.

Indeed, the structure of both Section 222 and the Proposed Rules are fundamentally different from the Vermont statute at issue in *Sorrell*. In the latter, "Vermont made prescriber-identifying information available to an almost limitless audience," and its "explicit structure … allows the information to be studied and used by all but a narrow class of disfavored speakers."[42] In contrast, Section 222 broadly imposes a duty on telecommunications carriers to "protect the confidentiality" of customer information, and requires customer approval for the "use" or "disclosure" of such personal information in all but a limited set of exceptional situations. Likewise, the Proposed Rules generally require opt-in consent both for disclosures of customer information to third parties and for providers' own uses, creating a few specific exceptions

[39] *Sorrell*, 564 U.S. at 564–566.
[40] *Id.* at 566.
[41] *Id.*
[42] *Id.* at 572.

allowing implied or opt-out consent as a substitute for opt-in.[43] Thus, both the statute and the Proposed Rules reflect the sort of "more coherent" scheme to which *Sorrell* referred approvingly, "allowing the information's sale or disclosure in only a few narrow and well-justified circumstances," such as in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[44]

Furthermore, in allowing opt-out consent for a provider's own marketing of "communications-related services" while still requiring opt-in consent for marketing of all other services and uses, the Proposed Rules would limit the more stringent application of the latter to the particular circumstances where reasonable customer expectations and other considerations demand it.[45] This is exactly the sort of tailoring called for in *U.S. West Communications, Inc. v. FCC* and other First Amendment cases.[46] It would be nonsensical to find a "content-based" distinction in the FCC's attempts to more narrowly tailor opt-in requirements, and therefore apply a higher level of scrutiny.

B. The Heightened Scrutiny Framework Proposed By Opponents Would Call Into Question Section 222(b) and Is Inconsistent With Other Congressional Privacy Regimes That Have Survived Judicial Scrutiny.

In their complaints about purported content-based distinctions prohibited by the First Amendment, ISP commenters have largely argued that the Proposed Rules themselves are unconstitutional, as opposed to the underlying statutes. However, Section 222(b) also makes content distinctions, in restricting a carrier's use of customer information received from another carrier in the course of providing service to only "such purpose," while expressly forbidding any

[43] NPRM ¶ 18.
[44] *Id.* at 573.
[45] *E.g.*, NPRM ¶ 18.
[46] 182 F.3d 1224 (10th Cir. 1999).

uses of such information for a carrier's "own marketing efforts."[47] This explicit restriction on a particular sort of economic activity—marketing—is far closer to the fact pattern in *Sorell* than the broad restrictions on any type of use or disclosure imposed by Section 222(a) (general duty to protect confidential information) and 222(c) (specific duty to protect customer CPNI). It is difficult to see how commenters' suggestions of heightened scrutiny would not sweep in this provision as well.[48]

Taken to its logical end, applying strict scrutiny to the Proposed Rules would likely require the same for a wide array of other existing privacy regulations, which impose different restrictions and requirements on the use and disclosure of personal information depending upon the underlying purpose of the use or disclosure. For example:

- The HIPAA Privacy Rule allows for the disclosure of "Protected Health Information" (PHI) for "treatment, payment, or health care operations" without express written consent,[49] but requires such consent for other uses and disclosures.[50] In addition, HIPAA regulations require authorization for the use or disclosure of PHI for "marketing," but make certain exceptions for particular forms of marketing (e.g., making a "promotional gift of nominal value").[51]
- The Federal Education Rights and Privacy Act generally prevents educational institutions receiving federal funds from releasing education records without written parental consent, but permits disclosures without consent for a wide variety of purposes, such as

[47] 47 U.S.C. § 222(b).
[48] *Cf. Verizon California, Inc., supra* note 6.
[49] 45 C.F.R. § 164.506(a)
[50] 45 C.F.R. § 164.508(a)(1).
[51] 45 C.F.R. § 164.508(a)(3).

"conducting studies … for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction."[52]

- The Video Privacy Protection Act prohibits a "video tape service provider" from disclosing customer information to third parties absent affirmative written consent, but requires only opt-out consent to disclose customer names, addresses, and the "subject matter" of customer video rentals "for the exclusive use of marketing goods and services directly to the customer."[53]

All of these regulations may be vulnerable to challenge under an interpretation of the First Amendment that condemns any content-based distinctions found in commercial regulations. But this reasoning proves too much. In the absence of distinctions that are either intended to suppress particular messages or ideas or actually do so, there is no reason to apply broad strict scrutiny to all privacy protections. [54]

C. To Avoid Any Question of Content-Based Distinctions, the Commission Should Require Opt-In Consent For All Uses.

As explained above, the few exceptions to overarching opt-in requirements in the Proposed Rules would not transform them into content-based speech regulation warranting heightened scrutiny. However, to avoid any risk that a court would disagree, the Commission can avoid the question entirely by adopting a uniform opt-in requirement for all uses and disclosures of customer information. Public Knowledge has previously advocated for this approach, which reflects both the plain language of Section 222(c)(1)'s requirement and the

[52] 20 U.S.C. § 1232g(b)(1).
[53] 18 U.S.C. § 2710(b)(2)(D).
[54] *See* Neil Richards, "Why Data Privacy Law is (Mostly) Constitutional," 56 Wm. & Mary L. Rev. 1501 (2015).

uncertainty of opt-out consent as a reflection of actual customer approval.[55] And by simplifying potential constitutional challenges, uniform opt-in is a natural response to the arguments of commenters who now complain about purported content-based distinctions in the Proposed Rules.

III. The FCC's Proposed Rules Satisfy the Requirements of the Central Hudson Framework.

Under the *Central Hudson* framework, a restriction on commercial speech must satisfy three essential requirements: the "governmental interest [must be] substantial"; the regulation must "directly advance[ ] the governmental interest asserted"; and the regulation must not be "more extensive than is necessary to serve that interest."[56] The FCC's Proposed Rules would satisfy each of these requirements, and commenters' primary arguments to the contrary are without merit.

First, various commenters challenge the existence of a substantial governmental interest to justify the proposed opt-in regime. But it is beyond dispute that the government has a powerful interest in allowing consumers to determine for themselves "when, how and to whom personal information will be disclosed to others."[57] "The Supreme Court knows this as well as Congress: both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[58]

Even while conceding that this interest justifies the restriction of customer information to third parties, certain commenters argue that the government has no interest in the regulation of an ISP's own use of data gathered from their customers. This contention overlooks the

---

[55] Comments of Public Knowledge at 31.
[56] *Central Hudson*, 447 U.S. at 556.
[57] *NCTA*, 555 F.3d at 354.
[58] *Id.*; *see also Bartnicki v. Vopper*, 532 U.S. 514, 533–35 (2001).

practicalities of commercial use of customer data. Just as "common sense supports the Commission's determination that the risk of unauthorized disclosure of customer information increases with the number of entities possessing it,"[59] so too does the risk of unauthorized disclosure increase as sensitive information is disseminated within large organizations, especially when used for purposes beyond and unrelated to a customer's pre-existing service. Furthermore, the record already contains plentiful evidence of the potential and actual harms that result from unrestricted use of customer data by a customer's own BIAS provider, even where the data is never transferred to a third party.[60]

Certain commenters rely on the Tenth Circuit's decision in *U.S. West* to argue that the FCC cannot point to a substantial governmental interest to justify the opt-in requirements of the Proposes Rules. However, the decision in that case was focused entirely on the thinness of the administrative record, coupled with apparently deficient pleading and argumentation. This lack of evidence was determinative in every prong of the court's analysis, and the stated governmental interest failed because the court "prefer[red] to see a more empirical explanation and justification for the government's asserted interest."[61] Similarly, the court rejected the FCC's narrow tailoring argument not because they believed more targeted rules would be more effective, but simply because "the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy."[62] The court's holding was not a rejection of opt-in customer privacy rules (let alone of the FCC's constitutional authority to make such

---

[59] *NCTA*, 555 F.3d at 1001–02.
[60] *See* Charles Duhigg, *How Companies Learn Your Secrets*, The New York Times Magazine (Feb. 16, 2012), *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html; Open Technology Institute Comments at 26, note 65. (discussing potential application of first-party data for anticompetitive targeted advertising).
[61] *U.S. West*, 182 F.3d at 1234.
[62] *Id.* at 1237–38.

rules), but instead simply found an insufficient record to satisfy the requirements of *Central Hudson*. Given the size and scope of the current proceeding (including over a thousand pages of first-round comments and a 500-question NPRM), a repetition of these shortcomings is unlikely.

Second, various commenters dispute whether the Proposed Rules would directly advance the government's interests in allowing consumers to control their own personal information. In particular, several commenters have argued that the Proposed Rules are fatally under-inclusive, as they fail to regulate "other Internet companies … that have access to as much or more customer data than ISPs and have an outsized presence in the online advertising market."[63] As an initial matter, it appears that these commenters' ire lies with Section 222 itself, and its application of specific privacy requirements upon telecommunications providers. And in any event, the *Central Hudson* framework does not require regulatory efforts to be universally comprehensive, or to alleviate every potential source of a given harm. "A regulation is not fatally underinclusive simply because an alternative regulation, which would restrict more speech or the speech of more people, could be more effective."[64] Instead, "a rule is struck for underinclusiveness only if it cannot fairly be said to advance any genuinely substantial governmental interest."[65] The Proposed Rules follow the general opt-in approach under Section 222 that was approved by the D.C. Circuit in *NCTA*.[66] No commenter can seriously dispute the fact that imposing effective controls for personal data held by BIAS providers materially advances consumer privacy. The record contains extensive evidence that customer data

[63] *E.g.*, Tribe & Massey at 22.
[64] *Trans Union Corp. v F.T.C.*, 267 F.3d 1138, 1143 (D.C. Cir. 2001).
[65] *Id.*
[66] 555 F.3d at 1002.

collected by ISPs is uniquely sensitive, and raises more acute concerns than data collected by edge providers.[67]

Although several commenters claim that the Proposed Rules "single out"[68] BIAS providers while deliberately "excluding"[69] edge providers and others from regulation, this is simply not the case. Just as the Proposed Rules would restrict an ISP from using customer data, absent opt-in, for the marketing of non-communications-related services, they would also restrict disclosure of the same information to a third party company for the same purpose. If anything, the Proposed Rules are more permissive for ISPs than for third parties, as they allow opt-out consent for certain uses by the former while requiring opt-in consent for all instances of sharing with the latter. Additionally, nothing in the Proposed Rules would prevent ISPs or their affiliates from using other lawful sources of customer data, not acquired through their own provision of broadband service, for marketing or any other activity.[70] For example, an online advertising service owned and/or operated by an ISP could still make use of customer data obtained from edge providers to the same extent as a third party advertising service.

Finally, various commenters contend that the opt-in regime of the Proposed Rules is "more extensive than necessary" to serve the government's legitimate interest in protecting customer privacy.[71] For example, Comcast argues that the Proposed Rules would impose "the most onerous possible limitations on the use of this information and on the broadest definition of

---

[67] *See* Public Knowledge, Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World (Feb. 2016) at 45-57, available at https://www.publicknowledge.org/documents/protecting-privacy-promoting-competition-white-paper; Comments of Public Knowledge at 17-24.
[68] Tribe & Massey at 23.
[69] Comments of Comcast at 94–95.
[70] *See* NPRM ¶ 39 (proposing to limit the definition of CPNI to that which "the BIAS provider collects or accesses in connection with the provision of BIAS").
[71] *NCTA*, 555 F.3d at 1000 (quoting *Central Hudson*, 447 U.S. at 556).

covered customer proprietary information," and that the FTC's opt-out regime would be "significantly less speech-suppressing.[72] However, these arguments overstate the tailoring required in the *Central Hudson* framework. "The government is not required to employ the least restrictive means conceivable"—it need only demonstrate "a fit that is not necessarily perfect, but reasonable; that represents not the single best disposition but one whose scope is in proportion to the interest served."[73] Thus, "the government does not have to show that it has adopted the least restrictive means for bringing about its regulatory objective."[74]

As the D.C. Circuit has previously found in considering Commission implementation of Section 222, "opt-out is only 'marginally less intrusive' than opt-in for First Amendment purposes."[75] As long as the FCC "carefully consider[s] the differences between these two regulatory approaches," the court has "not require[d] exhaustive evidence documenting the necessity of opt-in over opt-out," deferring instead to "Congress's reasonable, commonsense determination that express customer consent was required."[76] And there is already ample evidence in the record to demonstrate the practical necessity of opt-in consent to protect sensitive customer information collected by BIAS providers.

Note also that, in portraying the FTC's privacy framework as a superior alternative to the Proposed Rules, several commenters have embraced the same type of "content-based" distinctions that they condemn elsewhere as violations of the First Amendment.[77] While the FTC framework generally allows first-party marketing based upon the use of data from a company's own customers, and permits opt-out consent for most other uses and disclosures of

---

[72] Comments of Comcast at 99.
[73] *Greater New Orleans Broad. Ass'n v. United States*, 527 U.S. 173, 188 (1999)
[74] *NCTA*, 555 F.3d at 1002.
[75] *Id.*
[76] *Id.*
[77] *See, e.g.*, Tribe & Massey at 33–34.

customer data, it requires opt-in consent for certain specific categories of "sensitive data," such as information about children, financial and health information, and geolocation data.[78] At a minimum, this contradiction shows how legitimate regulations of commercial practices to protect consumer privacy cannot avoid distinctions based on "content," and makes clear that heightened scrutiny should only be applied to regulations that target particular messages or speakers for "disfavored [or favored] treatment."[79]

IV. The FCC Should Reject Interpretations of the First Amendment as a Broad Bulwark against Legitimate Commercial Regulation.

In applying the particular doctrines for commercial speech and content neutrality to the Proposed Rules, the FCC should not lose sight of the broader context and purposes of the First Amendment. Broadband customers use their internet connections as a platform for their own speech—indeed, this is the service's basic purpose.[80] Without effective privacy protections, internet users may be forced to choose between this expressive activity and control over a significant amount of personal data. The Supreme Court has expressly recognized the government's "important interest" in the "[p]rivacy of communication," to encourage "the uninhibited exchange of ideas and information" that is a central goal of the First Amendment.[81] This privacy "is essential if citizens are to think and act creatively and constructively," and the "[f]ear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas."[82] Recent data confirms that privacy concerns have had exactly this effect,

---

[78] *Id.*
[79] *Sorrell*, 564 U.S. at 564.
[80] *See United States Telecom Ass'n v. FCC*, ___ F.3d ___, 2016 WL 3251234, *42–*44 (D.C. Cir. June 14, 2016).
[81] *Bartnicki*, 532 U.S. at 532.
[82] *Id.* at 533.

deterring substantial numbers of Americans from wider online activity.[83] Thus, privacy protections go hand in hand with the First Amendment rights of broadband customers as speakers and participants in "public discourse."[84]

To the extent commercial practices receive First Amendment protection at all, it is to protect the interests of listeners in receiving information, rather than the right of commercial actors to speak freely.[85] In *Central Hudson*, for example, the Court explained that "[t]he First Amendment's concern for commercial speech is based on the informational function of advertising."[86] This foundation for commercial speech protections suggests that opt-in requirements for the use of customer data in marketing data are generally consistent with listeners' interests in receiving information via commercial speech, because such regulations give individuals the right to receive such communications as desired.

More generally, the Commission should cast a skeptical eye on expansive theories of free speech protection for what are essentially commercial practices. For example, even if the Commission concludes that certain applications of the Proposed Rules do trigger at least some level of First Amendment scrutiny, it should take care not to embrace the amorphous notion that

---

[83] *See* Rafi Goldberg, "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities" (National Telecommunications & Information Administration, May 13, 2016), available at https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities; Lee Rainie, "How Americans balance privacy concerns with sharing personal information: 5 key findings" (Pew Research Center, Jan. 14, 2016), available at http://www.pewresearch.org/fact-tank/2016/01/14/key-findings-privacy-information-sharing/; Lee Rainie and Shiva Maniam, "Americans feel the tension between privacy and security concerns" (Pew Research Center, Feb. 19, 2016), available at http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/.

[84] *Snyder v. Phelps*, 562 U.S. 443, 460 (2011).

[85] *See* Amanda Shanor & Robert Post, "Adam Smith's First Amendment," 128 Harv. L. Rev. F. 165 (Mar. 16, 2015).

[86] *Central Hudson*, 447 U.S. at 563.

all data and information flows amount to constitutionally-protected speech.[87] Such arguments run the risk of immunizing large portions of the information economy from effective regulation.[88] "At best," this approach "opens a Pandora's Box of First Amendment challenges to many ordinary regulatory practices that may only incidentally affect a commercial message. At worst, it reawakens Lochner's pre-New Deal threat of substituting judicial for democratic decisionmaking where ordinary economic regulation is at issue."[89]

CONCLUSION

Although, as noted in its initial comments, the Commission's proposed rules could be improved, the objections raised by opponents lack merit. For the last 90 years, Congress has sought to empower users of electronic communications services to control the information related to these communications. This substantial government purpose has become more vital in the broadband world, where the inability of consumers to control their broadband data directly impedes their adoption and use of broadband. The rules proposed by the Commission, like Section 222 itself, are content neutral and thus subject only to the familiar analysis of commercial speech under *Central Hudson*.

---

[87] *See* Neil Richards, Reconciling Data Privacy and the First Amendment, 52 U.C.L.A. L. Rev. 1149, 1168–75 (2005) (arguing that the "suggestion that all privacy rules are speech rules is significantly overblown"); Richards, 56 Wm. & Mary L. Rev. at 1524–1528 (criticizing the "data-is-speech" argument). In defense of such theories, certain commenters point to Sorrell, claiming that the Court held that "the creation and dissemination of information are speech within the meaning of the First Amendment." Tribe & Massey at 13 (quoting *Sorrell*, 564 U.S. at 570. However, *Sorrell* went on to clarify that its holding was not actually so broad, as it rejected the challenged statute "even assuming, as the State argues, that prescriber-identifying information is a mere commodity." *Id.* at 571; *see also Richards*, 56 Wm. & Mary L. Rev. at 1521–24 (arguing for a narrower reading of Sorrell).

[88] *Id.* at 1529–1531.

[89] *Sorrell*, 131 S. Ct. 2653, 2685 (2011) (Breyer, J., dissenting).

For these reasons, the Commission should reject the arguments advanced by the anti-privacy commentors and move swiftly to adopt rules that will protect and empower consumers as Congress directed.

Respectfully Submitted,

/s/ Ryan Clough
General Counsel
Public Knowledge

/s/Jeffrey Chester
Executive Director
Center for Digital Democracy

/s/Richard Holober
Executive Director
Consumer Federation of California

/s/ Amina Fazlulah
Director of Policy
Benton Foundation

/s/Pam Dixon
Executive Director
World Privacy Forum

/s/ Linda Sherry
Director, National Priorities
Consumer Action

/s/John Breyault
Vice President of Public Policy, Telecommunications, and Fraud
National Consumers League

/s/Susan Grant
Director of Consumer Protection and Privacy
Consumer Federation of America

/s/Beth Givens
Executive Director
Privacy Rights Clearinghouse