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

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

REPLY COMMENTS OF FREE PRESS

Gaurav Laroia, Policy Counsel
Matthew F. Wood, Policy Director
Free Press
1025 Connecticut Avenue, N.W.
Suite 1110
Washington, D.C. 20036
202-265-1490

July 6, 2016

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY

Opponents of the FCC's privacy NPRM present a case that rests on several flawed premises and fallacies. These parties fundamentally misread Section 222. They purposefully conflate broadband ISPs having to ask users for consent, before sharing or using personal and proprietary information for marketing, with outright marketing bans. They vastly overstate the speech and compliance burdens for broadband ISPs should they have to gain such "approval of the customer"[1] in order to use their personal and proprietary information for marketing purposes. These privacy opponents are wrong about several other things too: the scope of the FCC's authority, especially in light of the D.C. Circuit's affirmance of the *Open Internet Order*; the unique responsibilities of common carriers in American law; the role of ISPs in the internet "ecosystem"; and the details of Commission's proposal itself.

As Free Press wrote in our initial comments, the logic of the Commission's proposal is inexorable.[2] If broadband ISPs are telecom carriers (and they are),[3] then these privacy provisions in Title II ought to apply (and they do). The application of such privacy protections to common carriers and the communications network is not new. It is sound policy that reaches back to the founding of the Republic.[4]

---

[1] *See* 47 U.S.C. § 222(c)(1).
[2] Comments of Free Press, WC Docket No. 16-106 (filed May 27, 2016) ("Free Press Comments").
[3] *U.S. Telecom Ass'n v. FCC*, No. 15-1063 (D.C. Cir. June 14, 2016) ("*USTA v. FCC*").
[4] *See generally* Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 Stan. L. Rev. 553, 568 (2007) (noting that the duties of communications carriers, including the duty to protect privacy, are deeply embedded in U.S. statutory law). Section 222's edict that telecommunications providers protect their customers' privacy is a reflection of this longstanding policy.

The conflation of telecom services and information services is the faulty foundation upon which many of these broadband industry arguments rest. ISPs' complaints about unfairness, and about over- and under- inclusiveness, stand on this same shaky base. Confusing ISPs with information service providers on the "edge" of the network is like confusing telephone carriers with individuals or corporations on either side of the line. It's wrong, both as a matter of policy and a matter of law.

The FCC's proposal – and the weight of the record evidence in this docket, once these unfounded ISP apologetics are discounted – all point the right way. The FCC's focus on broadband provider practices does not mean in any way, shape, or form, that edge providers are no threat to privacy. Yet that focus is entirely proper because Congress could quite rationally write a law to preserve longstanding protections for carriers' customers. And not only could Congress choose to do so; here, in fact, it did just that. The FCC must implement that law – not ignore it while waiting for a new one that applies to the whole "ecosystem," nor stretch it to apply to services clearly outside of the Commission's jurisdiction under Title II.

Thus, the FCC's proposal does not single out any companies improperly. It follows a straightforward congressional mandate to promulgate sector-specific privacy protections for broadband carriers. No confusing (and now debunked) claims about how much or how little of our data ISPs can "see," in comparison to other internet companies, changes this statutory imperative to safeguard carrier customers' data.[5]

[5] *See* Peter Swire, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, at 7 (Feb. 29, 2016) ("*Swire Report*").

Ultimately, the Commission's proposal is lawful and essential. It passes both statutory and constitutional muster. Though not properly subject to any such level of scrutiny from a constitutional standpoint, these proposed rules will serve a compelling interest: protecting broadband users' privacy from unpermitted carrier intrusions, and enhancing users' trust in the indispensible communications network of our age.

I. THE COMMISSION HAS THE AUTHORITY TO ADOPT THE PROPOSED REGULATIONS.

A. Broadband ISPs are Title II Telecom Carriers Subject to the Mandates of Section 222.

As Free Press described in our initial comments, this proceeding is not an opportunity to re-litigate the *Open Internet Order*. At least some broadband providers agreed with this to a point, and were willing to accept the FCC's reclassification of BIAS providers under Title II *arguendo*.[6] Nevertheless, the arguing is now over. It is important to recognize the impact, once and for all in this proceeding, of the D.C. Circuit's affirmance of the Commission's *Open Internet Order* and reclassification decision. All members of the panel agreed the FCC has the statutory authority to reclassify broadband ISPs as telecommunications carriers.[7] That decision followed the lead of the Supreme Court's *Brand X* decision a decade earlier, deferring to the FCC's interpretation of the classification question.[8] With the current Supreme Court unlikely to hear a further appeal,[9] the status of broadband ISPs as Title II common carriers is settled law.

---

[6] *See, e.g.*, Comments of Comcast Corporation, WC Docket No. 16-106 at 94 (filed May 27, 2016) ("Comcast Comments).

[7] *See USTA v. FCC*, No. 15-1063, at 29.

[8] *See Nat'l Cable & Telecommunications Ass'n v. Brand X Internet Services*, 545 U.S. 967, 991 (2005).

[9] *See* Emily Hong & Sarah Morris, *Will the Supreme Court Really Take on Net Neutrality?*, Slate, June 16, 2016, http://www.slate.com/blogs/future_tense/2016/06/16/will_the_supreme_court_really_take_on_net_neutrality.html.

Yet, even after accepting the premise (as they now must) that Title II applies to broadband providers, commenters such as CTIA,[10] Comcast,[11] AT&T[12] and others suggest for a variety of reasons that Section 222 still does not apply to broadband. They argue that the statute cannot be a basis to protect broadband users' privacy, claiming to no avail that it was meant to apply solely to telephone companies. This reading of Section 222 is entirely implausible. Congress set out duties in Section 222 for all "telecommunications carrier[s]" under Title II of the Communications Act. If Congress meant to say "telephone companies," it certainly knew how to do so. In fact, a few subsections in Section 222 do establish specific duties for any "telecommunications carrier that provides telephone exchange service."[13] The mandates in subsections (a) and (c) are broader than that, and on their face apply to all telecom carriers (as they should). It is abundantly clear that all telecom carriers, including broadband providers, are now bound by law to protect their customers' privacy.

CTIA's manipulations of the statute are particularly egregious in this regard. CTIA suggests that the absence of words such as "access to the internet" in Section 222 preclude the application of the statute to telecommunications services that do indeed provide such access to the internet. But instead of reading the statute for what is not there, and guessing as CTIA does at the supposed meaning of the imagined omission, the FCC

---

[10] *See* Comments of CTIA, WC Docket No. 16-106, at 15 (filed May 26, 2016) ("CTIA Comments").
[11] *See* Comcast Comments at 67.
[12] *See* Comments of AT&T, WC Docket No. 16-106, at 101 (filed May 27, 2016) ("AT&T Comments").
[13] *See, e.g.*, 47 U.S.C. § 222(g); *see also* CTIA Comments at 16-17 (noting that several subsections in Section 222 refer to telephone and voice services, but critically failing to explain how these subsections "foreclose" application of the statute to other "telecommunications carriers.").

can and should simply read the statute as it stands. Both at the time Section 222 was written, and today in the wake of the D.C. Circuit's affirmance of reclassification, the term "telecommunications carrier" includes providers of services other than telephony.

B. The FCC Correctly Proposed a Comprehensive List of Information Covered Under Section 222.

The statutory sleight-of-hand by ISPs and their trade associations does not end with this attempt to make the broad term "telecommunications carrier" vanish from the face of the statute, and to have the term "telephone" appear in its place. CTIA and others should know that particular statutory language is not to be construed as "mere surplusage" when it appears in the text, and that different terms mean different things.[14] In fact, CTIA aptly demonstrated its desire to read every word in Section 222, finding deep meaning not just in the words that actually appear there but – somewhat more surprisingly – even in words that do not appear.[15]

Continuing its oddly mystical bent, CTIA offers some strange and pseudo-scientific advice when it encounters the different terms "proprietary information" (or "PI") in Section 222(a) and "customer proprietary network information" (or "CPNI") in Section 222(c). The wireless lobby counsels the Commission against "atomistic interpretation of Section 222(a)" and urges instead a "holistic[ ]" approach to the statute.[16] Now a careful reader of CTIA's comments might wonder where the lobby's "holistic[ ]" approach was less than ten pages prior, when it advised the Commission to

[14] *See Bailey v. United States*, 516 U.S. 137, 146 (1995) ("We assume that Congress used two terms because it intended each term to have a particular, nonsuperfluous meaning.").
[15] *See* CTIA Comments at 16-19.
[16] CTIA Comments at 25.

ignore the entirety of the statute in favor of focusing on "atomistic" references to telephone and voice services.

But in examining the plain text and meaning of the two different terms in subsections (a) and (c), it is clear that they mean two different things. The "proprietary information" category established in subsection (a) is broader than just CPNI. Commenters like the Open Technology Institute and EFF rightly contend that these are "related" but "distinct" obligations[17]; and that later, more specific prohibitions in Section 222 do not limit subsection (a)'s requirements for PI "but rather address specific obligations and exceptions in addition to that general duty to protect confidential customer information."[18]

C. That Edge Providers May Have Access to Certain Kinds of "Proprietary Information" Is Immaterial to Whether the FCC Can Protect The Use of That Information by Broadband ISPs.

AT&T suffers from a different but related strain of flawed statutory reading than the variety afflicting its trade groups. AT&T argues, citing Black's Law Dictionary, that information freely available to the public cannot be "proprietary," and therefore that Section 222(a) cannot include customer PI potentially available to third parties from other sources.[19] Yet this law dictionary definition actually refutes AT&T's argument rather than supporting it.

---

[17] Comments of New America's Open Technology Institute, WC Docket Nos. 16-106, 13-306, at 18 (filed May 27, 2016).
[18] Comments of The Electronic Frontier Foundation, WC Docket No. 16-106, at 2 (filed May 27, 2016).
[19] *See* AT&T Comments at 101 ("[T]o be proprietary, information cannot be freely available to the public; it must be kept confidential.").

The FCC proposes to define "proprietary information" as data that includes personally identifiable information "linked or linkable to an individual."[20] In a non-exhaustive list, the FCC includes the following examples of such information: Name; Social Security Number; physical and online addresses; internet browsing history; geo-location information; race; sexual identity; health information; and other types of personal data.[21]

AT&T contends that unlike in the telephone era, some of this personally identifiable information and even broadband CPNI may be available to "unregulated third parties" including a broadband user's "browser (e.g., Google Chrome), the search engine (e.g., Google), the webpage (e.g., Amazon), the content delivery network serving the webpage (e.g., Akamai), and any number of data brokers (e.g., Acxiom) that sell the end user's online information to others."[22] In other words, AT&T argues that since some other entities may have access to users' personally identifiable information at some times, AT&T's customers no longer have any proprietary right to that information.

By this reasoning, only secrets could ever be "proprietary." The law dictionary that AT&T cites offers no such cramped reading of the term proprietary, focusing instead on the "protective interest" that the "owner" of that information has in it. Neither is this information "readily available in public sources"[23] merely because some other entities involved in processing an online communication may have access to it.

---

[20] *See In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, ¶ 60 (2016) ("NPRM").
[21] *Id.* ¶ 62.
[22] AT&T Comments at 101.
[23] *Id.* at 101 n.209.

ISPs like AT&T and Comcast still insist that because other internet companies may have access to some of the same information as broadband providers, these two types of entities should be regulated in exactly the same way.[24] The argument that both network operators and information service providers must be regulated in the same manner is plainly self-serving, and wrong for all of the reasons outlined above. Congress can and did fashion separate protections for carriers' customers – not because users of the network like edge providers are not capable of violating other users' privacy, but because carriers are capable of doing so.

This self-serving argument and quest for false equivalence finds no support in the supposition that proprietary information means only information unknown to anyone else but the ISP. Neither Sections 222(a), 222(c), and 222(h) nor the plain meaning of the term "proprietary" dictate such an absurd result.

D. The *Swire Report* does not Support the Assertion That ISPs Have No Unique Insights Into Customer Activities.

Peter Swire's report on online privacy infects several broadband providers' arguments with clearly rebuttable claims about online encryption, about the prevalence of VPNs, and about the ability of ISPs to monitor their customers' online activity.[25] Broadband industry commenters repeatedly cite the report to buttress their claims about ISPs' limited access to their customer's information – first and foremost fixating on Swire's contention that soon 70% of internet traffic will be encrypted.[26] This statistic is

[24] *See, e.g.*, Comcast Comments at 7.
[25] *See Swire Report* at 7-8.
[26] *See, e.g.*, CTIA comments at 7; AT&T Comments at 11; Comcast Comments at 29; Comments of Verizon, WC Docket No. 16-106, at 21 (filed May 27, 2016) ("Verizon Comments"); Comments of T-Mobile USA, Inc., WC Docket No. 16-106, at 6 (filed May 27, 2016) ("T-Mobile Comments").

grossly misleading. As the technologists at Upturn deftly noted when analyzing Swire's arguments, "sensitivity doesn't depend on volume."[27] That 70% of total traffic figure is largely meaningless, because it includes encrypted traffic from video sites such as Netflix. While the video streaming that makes up a large percentage of overall internet traffic may indeed be encrypted other internet uses remain entirely unencrypted, including data from health destinations like WebMD, from political and religious sites, and from sites that could reveal personal information about children in a household.[28]

Commercial surveillance of any such unencrypted traffic can reveal a treasure trove of sensitive information about a person's finances, politics, religion, and sexuality. The privacy interest that users have in protecting that information is not lessened by the availability of technical tools, especially in light of the relatively slow and incomplete adoption of VPNs, and the relatively slow adoption of encryption for some types of content and some internet uses (like the much-anticipated internet of things).[29]

Furthermore, the availability of such self-help protections as encryption and VPNs does not (and should not) trump the statutory rights individuals have against unpermitted use of this information by the broadband providers they depend on for their connections to the internet. Upturn's analysis underscores this last point too, noting that even with encryption, "ISPs generally retain visibility into their subscribers' DNS

---

[27] *See* Upturn, "What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate," at 3 (Mar. 2016), *available at* https://www.teamupturn.com/reports/2016/what-isps-can-see.

[28] *Id.* at 3-4 ("[W]atching the full Ultra HD stream of *The Amazing Spider-Man* could generate more than 40GB of traffic, while retrieving the WebMD page for 'pancreatic cancer' generates less than 2MB. The page is 20,000 times less data by volume, but likely far more sensitive than the movie.").

[29] *See id.* at 4-6, 9.

queries" and know the sites they visit.[30] Lastly, as Upturn likewise notes, broadband providers can learn "a surprising amount about the contents of encrypted traffic without breaking or weakening encryption" simply by "examining the features of network traffic – like the size, timing and destination of the encrypted packets."[31] Returning to the video streaming example above, it does not require a great deal of detective work to guess the type of content involved in a two-hour long, high-volume encrypted session with Netflix or Amazon.

The *Swire Report* has done the industry no favors. It shows how precarious broadband user privacy is, and how broadband ISPs' network position gives them a broad view into their customers' online activities.

II. BROADBAND PRIVACY REGULATIONS WITHSTAND ANY FIRST AMENDMENT SCRUTINY.

Opponents of the FCC's proposal claim that these privacy safeguards would constitute a substantial and impermissible First Amendment burden, citing both the proposed opt-in framework and potential regulation of financial inducements (pay-for-privacy). These assertions are meritless.

The FCC's proposal does not prohibit "targeted" marketing to broadband customers by ISPs subject to these rules. Instead, the FCC proposes that such broadband providers merely ask their customers if the company is permitted to monitor, use, share, or sell the information that broadband customers cannot help but generate as they use the internet.

[30] *Id.* at 6-7.
[31] *Id.* at 8.

Protecting the privacy of information sent over common carrier telecommunications networks in this manner is longstanding U.S. policy – and for good reason. These networks are the backbone of the U.S. economy. They carry information regarding every conceivable human activity in modern society. Protecting the integrity of those networks, and guarding that information from abuse while preventing its commodification without the customer's permission, are laudable and sensible goals. That the technology gives telecom companies the processing power to sort and sell this information does not heighten the government's burden under the First Amendment.

Various broadband industry associations commissioned Professor Lawrence Tribe[32] to raise First Amendment concerns, chiefly but not exclusively following the test set out in *Central Hudson*. His filing argues that the government cannot demonstrate a substantial interest in protecting broadband privacy; that the FCC impermissibly "singles out" broadband ISPs for onerous speech restrictions; and that it would unduly burden ISPs by requiring them to obtain opt-in consent. All of these assertions are false and based on fundamental misunderstandings of the FCC's proposal. The privacy interests at stake are substantial, to say the least, and the supposed constitutional burdens created by the Commission's proposed regulations are minimal at most.

A. The FCC's Proposal Does Not Trigger The First Amendment Concerns That ISPs Suppose.

Professor Tribe looks to the 10th Circuit's finding in *US West, Inc. v. FCC*[33] to buttress his claim that there are serious First Amendment rights at stake in this

[32] Joint Comments of CTIA, NCTA and USTelecom, "The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate The First Amendment," WC Docket No. 16-106 (filed May 27, 2016) ("Tribe Comments").
[33] See *US West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999).

proceeding. The *US West* court held that "a restriction on speech tailored to a particular audience, 'targeted speech,' cannot be cured simply by the fact that a speaker can speak to a larger indiscriminate audience, 'broadcast speech.'"[34] Yet there is no ban or real burden on tailored marketing on the table here.

As in it did in the *US West* case, the FCC merely proposes allowing the customer to decide whether she approves of her telecommunications carrier surveilling her telecommunications and using acquired proprietary information for marketing purposes. The rules proposed in this docket give that customer the opportunity to answer in the affirmative should she so choose, or in the negative instead.

If that customer chooses not to opt-in, the ISP is not properly understood to be barred from "speaking" to audiences it would prefer to target. Rather, requiring that a broadband provider obtain its customer's consent before speaking on these terms merely recognizes that even if ISPs have a right to engage in such commercial speech, they have no right to demand that their customers listen to it.

Tribe's strenuous efforts to make this user freedom into an ISP burden fail, because he casts ISPs as speakers but utterly fails to recognize customers' well established right not to listen. Citing the Supreme Court's 1943 decision in *Martin v. Struthers*, Tribe quotes language suggesting that laws may not burden speech by making the speaker a "a criminal trespasser" in the absence of "an explicit command from the owners to stay away."[35] A broadband customer's decision to withhold consent, by opting not to hear such speech from the ISP, is just such an "explicit command…to stay away." As the Court later recognized in *Frisby v. Schultz*, by way of distinguishing the *Martin*

[34] *Id.* at 1232.
[35] Tribe Comments at 10 (quoting *Martin v. Struthers*, 319 U.S. 141, 148 (1943)).

case Tribe so approvingly cites, "unwilling listeners may be protected when within their own homes."[36] Just so here: a broadband customer can refuse to accept any "such intrusion by an appropriate sign," such as withholding consent, because "[t]here simply is no right to force speech into the home of an unwilling listener."[37]

B. The FCC's Proposal Passes the *Central Hudson* Test.

Assuming *arguendo* that commercial speech issues are at stake in the NPRM, *Central Hudson* establishes a four-factor intermediate scrutiny test to determine whether the regulation survives constitutional scrutiny.[38]

1. If the speech concerns lawful activity and is not misleading, the reviewing court then asks:
2. whether the asserted government interest is substantial; and if so,
3. whether the regulation directly advances the government interest asserted; and
4. whether the regulation is not more extensive than necessary to service that interest.[39]

None of these individual prongs are definitive, and any regulation should be read in its totality to determine its constitutionality. That is because "the four parts of the *Central Hudson* test are not entirely discrete. All are important and, to a certain extent, interrelated: Each raises a relevant question that may not be dispositive to the First Amendment inquiry, but the answer to which may inform a judgment concerning the other three."[40]

---

[36] *Frisby v. Schultz*, 487 U.S. 474, 485 (1988).
[37] *Id.*
[38] *Central Hudson Gas and Electric Corp. v. New York Public Service Commission*, 447 U.S. 557 (1980).
[39] *Id.* at 566.
[40] *Greater New Orleans Broad. Ass'n v. United States*, 527 U.S. 173, 183-84 (1999).

Parties opposing the NPRM cite *Sorrell*[41] as precedent for applying an even higher standard to rules that impose so-called speaker-based restrictions on commercial speech. But the *Sorrell* decision's ambiguity "has made lower courts very cautious in abandoning, or even altering, the established intermediate-tier analysis."[42] Under the *Central Hudson* test, the NPRM would survive intermediate scrutiny (even if it were held to such a standard) because the government interest is substantial; the proposed regulations directly advance that interest; and the regulation is not more extensive than necessary.

C. There Is a Substantial Interest in Protecting Broadband Users' Privacy.

As Free Press noted in our initial comments, there are substantial interests at stake in protecting telecommunications privacy. In addition to avoiding the "disclosure of sensitive and potentially embarrassing personal information,"[43] there are substantial interests too in preventing data breaches; protecting against behaviors that limit economic opportunities for people of color and members of other communities subject to discrimination; preventing the unpermitted and undisclosed sale of personal information to data brokers; and protecting the dignity inherent in a person's right to control her own personal information. "The Supreme Court knows this as well as Congress: 'both the common law and the literal understandings of privacy encompass the individual's control

[41] *Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011).
[42] Oleg Shik, *The Central Hudson Zombie: For Better Or Worse, Intermediate Tier Review Survives* Sorrell v. IMS Health, 25 Fordham Intell. Prop. Media & Ent. L.J. 561, 563 (2015).
[43] *US West*, 182 F.3d at 1236.

of information concerning his or her person.'"[44] The FCC under Section 222 and related statutes has a direct and material interest in ensuring protection of such information.

ISPs focus on the harms associated with sharing customer PI with third parties, in an attempt to draw attention away from the substantial interest in protecting against broadband providers' own unpermitted use of such private information. AT&T, for example, finds no issue with first-party marketing because the consumer information used "remains confined to the ISP," and thus any restriction supposedly would "have no effect on access to the information."[45] Likewise, Verizon argues that the regulations purportedly "do not advance any substantial or compelling government interest."[46] Professor Tribe echoes these points arguing, that the government "promotes no discernible 'privacy' interest by keeping ISPs from merely using (rather than disclosing) information already in their possession to serve consumers with more rather than less relevant advertising."[47]

We are compelled to repeat ourselves. The FCC is not banning marketing, targeted or otherwise, to broadband ISP customers. Congress, in passing Section 222, recognized the right to choose how one's proprietary information may be used by the telecommunications carrier to whom it is disclosed in the course of providing "the telecommunications service from which such information is derived."[48] This right to control other uses by the ISP is an integral part of the privacy that the paying customers of these telecommunications carriers deserve under the statute.

---

[44] *NCTA v. FCC*, 555 F.3d 966, 1001 (D.C. Cir. 2009) (quoting *U.S. Dept. of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 763 (1989)).
[45] AT&T Comments at 94.
[46] Verizon Comments at 30 (emphasis in original).
[47] Tribe Comments at 20.
[48] 47 U.S.C. § 222(c)(1).

To further support its proposals and demonstrate the interests that it serves, the FCC relied in part on a Pew Research Center study that shows "the vast majority of adults deem it important to control who can get information about them,"[49] relying on the generally accepted understanding that "[i]ncreasing the number of entities that have access to customer PI logically increases the risk of unauthorized disclosure by both insiders and computer intrusion."[50] Verizon tries to counter the FCC's justification by stating that nothing in the Pew study "suggests that customers view an opt-out regime as insufficient to protect their information." However, even assuming that to be true, it does not negate the substantial interest. As Comcast conjectured, "people faced with an opt-in choice almost never opt-in,"[51] which supports the Pew Study finding that customers value their privacy. Giving broadband customers the tools with which to consent or not, and to effectuate that desire per Section 222's safeguards, is a substantial government interest.

D. The FCC Proposal Directly Advances the Government's Interest in Protecting Broadband Users' Privacy.

Central Hudson's second prong is easily met by the FCC. Congress wanted telecommunications carriers' customers to have a choice about whether their personal information would be used for purposes other than providing the telecommunications services they purchased. These proposed rules give them exactly that choice. The FCC proposes a requirement that all broadband providers "obtain customer opt-in approval before (1) using customer PI for purposes other than marketing communications-related service; (2) sharing customer PI with affiliates providing communications-related

[49] NPRM ¶ 129.
[50] *Id*. (see also *NCTA v. FCC*, 555 F.3d at 1001-02).
[51] Comcast Comments at 49.

services for purposes other than marketing those communications-related services; and (3) sharing customer PI with all other affiliates and third parties."[52]

Professor Tribe finds fault with the FCC's proposed rules, arguing that they are under-inclusive because they do not regulate edge providers. He disagrees with the FCC's finding that users have little choice among broadband providers. And he says that the rules do not differentiate between sensitive and non-sensitive information. These contentions are all easily dismissed, even when broadband providers and others repeatedly made these same errors when discussing the FCC's proposal.

Tribe writes, "the regulatory asymmetry between broadband ISPs and major digital platforms shows that the FCC's proposed rules are not tailored to any important governmental interest."[53] As we discussed above, broadband providers are not similarly situated with edge providers, nor is there any legal import to claims that they are part of the same internet "ecosystem." We detailed in Part I the rational and well-established basis for treating carriers differently, and for assuring that carriers' customers are protected from potential privacy invasions by carriers, though such assurances are not a panacea for other legitimate of privacy concerns.

What's more, there are several practical distinctions between carriers and edge providers. Users typically must pay broadband ISPs (exorbitantly[54]) for internet access. That is a different bargain than the one struck between many edge providers and their customers, and helps to yet again illustrate the rational basis for sector-specific rules that

[52] NPRM ¶ 127.
[53] Tribe Comments at 4.
[54] *See* Dana Floberg, Free Press, "Sky-High Prices Make Broadband Out of Reach for Many Low-Income Families," Jan. 8, 2016, *available at* http://www.freepress.net/blog/2016/01/08/sky-high-prices-make-broadband-out-reach-many-low-income-families.

govern carriers differently from users, even when some of those users are themselves large edge providers.

Broadband ISPs serve a separate function from the one served even by other large companies that use the internet themselves but do not provide internet access. Likewise, ISPs do not become part of the "healthcare ecosystem" when they provide internet access to hospitals, nor are they made part of the "banking ecosystem" by connecting a broadband customer on one end of the network to a bank on the other. It is only when these "internet companies" act as broadband providers that they would be subject to these FCC rules. If AT&T provides information services like email or search engines, it can do so outside the purview of these proposed rules for carriers. (Just as AT&T is free to open a bank or a hospital if it so desires.)

The converse is also true. Alphabet, Google's corporate parent, illustrates this clearly. When it provides broadband internet access service through Google Fiber, it is subject to the FCC's rules regarding common carriers. In its other incarnations, as a search engine, mapping service, or email provider, it is subject to FTC oversight. Calico, Alphabet's biotech research arm, is subject to sector-specific rules regarding healthcare and the sciences; and Google Capital is subject to rules regarding the financial industry. Though information technology connections exist between these various entities, it does not diminish the wisdom of sector-specific rules regarding their various activities, especially when it comes to privacy.

Professor Tribe trots out the exceptionally tired and false line that consumers have meaningful choice when it comes to broadband providers, and also suggests that encryption is sufficiently widespread to meaningfully protect broadband privacy. Citing

the *Swire Report* for both claims, Tribe writes that "the average internet user has 6.1 connected devices" that are "served by multiple ISPs," and says that "any one ISP today is therefore the conduit for only a fraction of a typical user's online activity and thus is not in a position to view more than a portion of that activity."[55]

Two wrong, ISP-paid pundits do not make a right, and Tribe's repetition of Swire's faulty analysis is no better than the original telling. First of all, the average number of connected devices that Swire takes from a Cisco report says nothing about the actual number of ISPs that serve the average internet user. For the purposes of broadband provider privacy, it does not matter if a user has three laptops, four mobile phones, and three more tablets if each of these devices connect to the same one or two ISPs. The relevant question is not how many devices a typical internet user has, but rather how many different ISPs the average user accesses, and whether or not any secondary ISPs are utilized in the same manner as the primary ISP.

According to Free Press's analysis of the most recent US Census Bureau Current Population Survey ("CPS") data, a full 99 percent of U.S. home internet users use just two ISPs at home, and the majority of those use only one.[56] This equates to the average person having 1.43 "home" access modes: their primary home ISP and/or their mobile carrier.[57] The CPS also asked internet users if they use the internet outside of the house

---

[55] Tribe Comments at 20 (citing *Swire Report* at 3, 34).

[56] Free Press analysis of data from "Current Population Survey, July 2015: Computer and Internet Use Supplement, conducted by the Bureau of the Census for the U.S. Department of Commerce, National Telecommunications and Information Administration." Of the 235 million Americans aged 3 and older that use the internet from home, 134 million report using just one ISP at home. Another 98 million report using two, with 99.6 percent of these two ISP-using persons accessing via mobile.

[57] *Id.* Of the 98 million of Americans aged 3 and older that report using the Internet at home from no more than two ISPs, 91 million report accessing the internet via their

(*e.g.*, at work, at school, in a cafe, at a library or community center, or in some other place). From this data we see that two-thirds of internet users age 3 and older use the internet at these other locations too. Among those who reported using one of the previously mentioned "home" ISPs, the average number of outside of the home locations was 1.6, with more than half accessing the internet at their workplace.[58]

Thus, from this data we have a clear picture of the average U.S. internet user: a person who subscribes to one home ISP and one mobile ISP at most, and who also goes online via one other method outside of the home (most often at work). This is hardly the ISP choice bonanza portrayed in the *Swire Report*. Furthermore, it is important to denote the difference in user perception of these out-of-home ISPs. Those who go online at work or school, or even at some other public access point, likely understand that these networks do not offer the same level of security and privacy as the users' home network. Indeed, many employers severely restrict the types of online activities and destinations their employees may access. And while the typical internet user has a mobile connection in addition to her home ISP, there's ample evidence that users conduct very different types of activities on wired versus mobile connections. Mobile connections are valued for their mobility; home connections are valued for their capacity.

---

mobile data plan outside of the home. Thus, the data confirms the expected norm: the average internet user goes online at home and via their mobile carrier outside of the home. In some cases, the same mobile data service is the sole connection used at and away from the home, while in other cases the wired home ISP is the same carrier providing the mobile service out of the home.

[58] *Id.* Of the 247 million of Americans aged 3 and older that use the internet from anywhere, 164 million report using the internet out of the home. Of these 164 million, the average number of outside locations used (amongst the 5 options of work, school, cafe, library/community center, or "other" place) is 1.56. 84 million of these 164 million persons say they go online at work.

While this data reveals that users are on average accessing the internet via just a few methods (and they overwhelmingly rely on their primary home connection), it also indicates that multiple-ISP access is a privilege of those who are more likely to be high-income, non-Hispanic whites. For example, only 46 percent of adult internet users in the lowest income quintile access the internet from work, versus 77 percent of top income quintile internet users.[59] And while 70 percent of white adult internet users report going online at work, only 56 percent of non-white adult internet users did.[60]

Swire's figures on encryption deployment across the web are repeated by Tribe here. We have dealt with them above in Part I. Suffice it to say again that many chat applications, websites, and others sources of information remain unencrypted, and even then ISPs can paint detailed pictures of their customers' lives by monitoring their CPNI. Tribe also claims that Virtual Private Networks provide additional protections by obscuring IP addresses. Even if this is true, VPNs are technologically sophisticated tools that require substantial time and money to operate. To claim that the FCC cannot show a substantial interest in protecting broadband users' privacy, just because some number of technologically sophisticated users can safeguard their own private information from their broadband providers, is unconscionable. It dismisses the privacy interests of poor and otherwise vulnerable users who may not have access to such tools, as well as the

[59] *Id.* For persons aged 18 and above. Income quintiles determined based on responses for family income.

[60] *Id.* In total, 66 percent of non-Hispanic whites (aged 3 and above) with home internet use the internet out of home, versus 62 percent of ethnic and racial minorities (aged 3 and above) with internet at home. Only 56 percent of bottom income quintile home internet users used the internet outside the home, versus 76 percent of top income quintile home internet users (all aged 3 and above).

privacy interests of less technologically savvy internet users who may not know about such tools. This is ivory tower elitism at its worst.

Finally, there is no truth to Tribe's claim that the FCC proposal fails this prong by not tailoring the proposal narrowly to "sensitive" data. This stipulation rests on a faulty premise: that sorting out what information is and is not sensitive when it comes to CPNI and PI is both technologically feasible and less privacy intrusive than bright-line rules.

As a customer generates PI and CPNI when they use their broadband provider's services, they may send unencrypted messages regarding personally identifiable information such as their health, their politics, their geo-location, and other data. To sequester health information from other information would require inspection of each packet crossing the network, and then require the ISP to make a determination about what is sensitive or not. This is analogous to asking a postal carrier to open each envelope so as to assess each letter's sensitivity, or asking a phone company to listen to each conversation to do the same. Paradoxically, such attempts to provide heightened protections against telecom carriers for some forms of information and not others would necessitate more and deeper surveillance of a customer's activities. A straightforward opt-in regime gives customers better ability to decide if they are comfortable having their internet use monitored by their ISP for marketing purposes.

E. The FCC's Approach Is "Not More Extensive Than Is Necessary" to Protect Broadband Customer Privacy.

Opponents of the FCC's proposed rules have suggested that adopting the FTC's "notice and choice" framework, and moving to an "opt-out" standard with regards to most information collection and sharing, would be more workable and less burdensome

than the FCC's proposal. Moving to such a model would have no such benefits, and the current FCC proposal is properly tailored to protect broadband customer privacy.

Professor Tribe praises three characteristics of the FTC's privacy framework and suggests that the FCC follow that approach:[61] he says thag implied consent should apply to first-party marketing for all services (not just telecommunications services) because such marketing is "within the expectation of the consumer"; that opt-in consent should be limited to "sensitive data" including information "about children, financial and health information, Social Security numbers, and certain geolocation data"; and that all other information should be subject to an opt-out consent mechanism.

This proposal defies consumer expectations, and it is unworkable too. Contrary to the assertion that consumers accept broad information sharing for marketing purposes when they purchase a service, the weight of the evidence shows that consumers are dissatisfied with the current state of affairs and increasingly upset about their lack of choice. According to a 2015 University of Pennsylvania study, 71% of respondents disagreed with the proposition that a physical store ought to be able to monitor a customer's internet activity in exchange for free wireless internet use.[62] 84% of respondents wanted more control over what marketers learned about their online activities, yet 65% have come to accept that individuals have little control over this. It is clear that consumers have deep concerns about the monitoring of their online activities. Their seeming resignation to this phenomenon should not be read as acceptance, nor

[61] Tribe Comments at 33.

[62] Joseph Turow, *et al.*, *The Tradeoff Fallacy: How Marketers are Misrepresenting Americans Consumers and Opening them up to Exploitation*, Annenberg School for Communication University of Pennsylvania, June 2015*, available at* https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

could such acceptance wipe away their privacy rights. Concerns about carriers' surveillance of our means of communications, and misuse of the information they acquire, are what drove Congress to pass Section 222 in the first place. Americans value this ability to choose how their personal information may be used. When it comes to telecommunications services, Congress thought it wise to effectuate that choice.

Tribe's breakdown of the opt-in/out framework betrays a weak understanding of broadband ISPs' bottleneck position in the network, and of the nature of the proposal itself. As we explained just above, any attempt by an ISP to sequester "sensitive" information discovered during a customer's internet use would necessitate a far more invasive and technologically sophisticated surveillance regime than a simple bright-line rule. The FCC proposes that customers be asked their privacy preferences at the point of sale.[63] Whether the question posed to the consumer is "do you opt-in to data monitoring for marketing purposes" or "do you opt-out of data monitoring for marketing purposes," the compliance burden for ISPs is the same. Indeed, the D.C. Circuit has previously found that "common sense" supported an FCC "determination that an opt-in consent requirement directly and materially advanced the interests in protecting customer privacy and in ensuring customer control over the information."[64] That case further found that the difference between opt-in and opt-out is only "marginal" for First Amendment purposes.[65]

[63] NPRM ¶¶ 82-83; *see also* proposed Section 64.7001.
[64] *NCTA*, 555 F.3d at 1001-1002
[65] *Id.* at 1002

The FCC proposal is not more expansive than necessary to effectuate its substantial interest. Despite arguments to the contrary,[66] the FCC's regulations need not be "perfect," but only "reasonable" and "in proportion to the interest served."[67] An "opt-in consent scheme presumes that consumers do not want their information shared unless they expressly indicate otherwise; an opt-out scheme … presumes the opposite."[68] As seen through the studies and facts on the record here, consumers choose to protect themselves better when given a clear opportunity to do so.

F. The FCC Has the Authority to Ban Coercive Financial Inducements Without Violating the First Amendment.

In our initial comments Free Press explained that the FCC has ample statutory authority to ban coercive or unfair terms, such as unfair financial inducements, under Sections 201(b) and 202(a) of the Communications Act.[69] Regulation of financial inducement schemes to protect consumers represents a substantial government interest, and rules effectuating such protections likewise withstand constitutional scrutiny.

The Commission acknowledges the common practice among businesses to offer consumers "perks in exchange for use of their personal information," but questions whether in the "broadband ecosystem … consumers generally understand that they are exchanging their information as part of those bargains."[70] The FCC further notes that the FTC has "argued that these business models unfairly disadvantage low income or other

---

[66] AT&T incorrectly interprets *Central Hudson* to require that the availability of a "less restrictive alternative bars the government from suppressing truthful commercial speech." AT&T Comment at 97. While the final prong of *Central Hudson* has been interpreted in a manner closer to strict scrutiny, this is not the law, nor a precedential requirement.
[67] *Bd. of Trustees of the State University of New York v. Fox*, 492 U.S. 469, 480 (1989).
[68] *NCTA*, 555 F.3d at 1002.
[69] Free Press Comments at 14.
[70] NPRM ¶ 260.

vulnerable populations who are unable to pay for more expensive, less-privacy invasive service options."[71]

Verizon argues that regulating broadband providers financial-inducement practices would implicate the First Amendment, because such rules would be based on "communicative content – namely, their power to persuade customers to agree to share their information"[72]; and would "burden customers' decisions to agree to the use and disclosure of their information to third parties."[73] As a result, Verizon believes the FCC proposal violates the "*Sorrell/Central Hudson* test … because it does not advance any substantial government interest and is not narrowly tailored."[74]

Though the Supreme Court has found blanket bans on the dissemination of truthful, non-misleading information about lawful activity to be overly inclusive in violation of the First Amendment,[75] combating misleading information satisfies the first prong of the *Central Hudson* test. There is a substantial government interest in protecting consumers from discriminatory, misleading, or exploitative behavior by telecommunications providers. By restricting any financial inducement practices of broadband providers that discriminate against targeted vulnerable populations, the FCC would directly further a substantial government interest, and could do so in a way that is no more extensive than necessary.

---

[71] *Id.*
[72] Verizon Comments at 51.
[73] *Id.* at 52.
[74] *Id*.
[75] *See* 44 *Liquormart v. Rhode Island*, 517 U.S. 484, 504-507 (1996); *Central Hudson*, 447 U.S. 557; *Carey v. Populations Services, Int'l*, 431 U.S. 678, 700 (1977).

CONCLUSION

Congress, in passing Section 222, made the correct policy determination that telecommunications providers have no business interfering with their customers' network traffic nor monitoring that traffic and commercializing it without their customers' consent. The Commission must follow through on this statutory mandate and do so without delay. The FCC should be confident in the knowledge that it is effectuating a substantial government interest and exercising its lawful authority to protect the open internet.

Respectfully Submitted,

/s/ Gaurav Laroia

Gaurav Laroia, Policy Counsel
Matthew F. Wood, Policy Director
Free Press
1025 Connecticut Avenue, N.W.
Suite 1110
Washington, D.C. 20036
202-265-1490

July 6, 2016